Operator Guide

VeloCloud SD-WAN 7.0

Version 7.0

Arista.com

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

Contents

Chapter 1: What's New..... 1

Chapter 2: About VeloCloud SD-WAN Operator Guide.....4

Chapter 3: Overview of VeloCloud Edge Cloud Orchestrator..... 5

Chapter 4: Supported Browsers.....6

Chapter 5: Log into the Orchestrator Using SSO for an Operator User.....7

Chapter 6: Configure the Advisory Notice and Consent Warning Message for Orchestrator..... 11

Chapter 7: Monitor Customers..... 13

Chapter 8: Manage Customers..... 15

8.1 Create a New Customer..... 16
8.2 Clone a Customer..... 21
8.3 Configure Customers..... 23
Configure SD-WAN..... 24
Configure Additional Settings..... 26
8.3.1 Configure a Handoff Operator..... 30
8.3.2 Configure Distributed Cost Calculation..... 37
8.3.3 Configure Path Calculation with Multiple DSCP Labels per Flow..... 40

Chapter 9: Manage Partners..... 43

9.1 Create a New Partner..... 44
9.2 Configure a Partner..... 46

Chapter 10: Partner Settings..... 49

Chapter 11: Manage Operators.....51

11.1 Monitor Operator Events..... 51
11.2 Manage Operator Profiles..... 52

Chapter 12: Link Insights..... 61

12.1 Executive Summary....64
12.2 Degradation Summary....64
12.3 Degradation Details....66

Chapter 13: User Management-Operator....68
13.1 Users....68
13.1.1 Add New User....69
13.1.2 API Tokens....71
13.2 Roles....73
13.2.1 Add Role....75
13.2.2 Enterprise Security Admin Role....76
13.3 Service Permissions....80
13.3.1 New Permission....83
13.3.2 List of User Privileges....85
13.4 Authentication....93
13.4.1 Time-Based One Time Passcode (TOTP)....105

Chapter 14: Orchestrator Branding for Operator....110

Chapter 15: Manage User Agreements....118

Chapter 16: Manage Gateway Pools and Gateways....122
16.1 Manage Gateway Pools....122
16.1.1 Create New Gateway Pool....124
16.1.2 Clone a Gateway Pool....125
16.1.3 Configure Gateway Pools....126
16.2 Manage Gateways....129
16.2.1 Create New Gateway....131
16.2.2 Configure Gateways....134
16.2.3 Upgrade Orchestrator for Dual Stack Support....139
16.2.4 Configure IPv6 Address on Gateways....139
16.2.5 Partner Gateways....141
16.2.6 Monitor Gateways....148
16.3 VeloCloud Gateway Migration....151
16.3.1 Limitations of VeloCloud Gateway Migration....153
16.3.2 Quiesce Gateways....154
16.3.3 Decommission Quiesced Gateways....155
16.4 Diagnostic Bundles for Gateways....156
16.4.1 Request Diagnostic Bundles for Gateways....156
16.4.2 Request Packet Capture Bundle for Gateways....158

Chapter 17: Platform and Modem Firmware and Factory Images....161

Chapter 18: Software Images....164

Chapter 19: Edge Licensing....166
19.1 Manage Edge Licenses for Partners....168
19.2 Manage Edge Licenses for Customers....169

Chapter 20: Application Maps....172

Chapter 21: Edge Management....177
Software & Firmware Images....178

Chapter 22: Access SD-WAN Edges Using Key-Based Authentication....180
22.1 Add SSH Key....180
22.2 Revoke SSH Keys....181
For Other Operator Users....182
22.3 Enable Secure Edge Access for an Enterprise....182
22.4 Secure Edge CLI Commands....182
22.4.1 Sample Outputs....185

Chapter 23: Configure User Account Details....188

Chapter 24: Orchestrator Diagnostics....193
Diagnostic Bundles....193
Requesting Diagnostic Bundle....194
Downloade a Diagnostic Bundle....195
Update Cleanup Date....195
Deleting a Diagnostic Bundle....195
Database Statistics....195

Chapter 25: Orchestrator Upgrade....198
Configure the Orchestrator Upgrade Announcement....198
Prepare the Orchestrator Upgrade....199
Complete the Orchestrator Upgrade....200

Chapter 26: Replication....202

Chapter 27: System Properties....203

Chapter 28: External Certificate Authority....205

Chapter 29: Appendix....215
29.1 Operator-Level Orchestrator Alerts and Events....215

Chapter 30: References....223
30.1 Related Documents....223

Chapter 1

What's New

Table 1: What's New in Version 7.0.0

Feature	Description
Kafka-Based Ingestion of Firewall Logs, Statistics, and Events	This feature introduces support for ingesting and storing firewall logs into Orchestrator ClickHouse (CH) tables through Kafka, for both on-premises and hosted deployments. This feature introduces the following two new system properties to control Kafka-based ingestion of firewall logs: • `vco.kafka.fwlogs.ingestion.enabled` • `vco.kafka.fwstats.ingestion.enabled` For more information, see the *List of System Properties* topic in the *VeloCloud Orchestrator Deployment and Monitoring Guide*.
Link Insights On-Prem Support	This feature enables continuous monitoring of link-level Quality of Experience (QoE) metrics, including latency, jitter, and packet loss. Link Insights identifies degraded connections and quantifies the effectiveness of SD-WAN optimization. For more information, see Link Insights. This feature introduces the following two new system properties: • `enterprise.capability.enableLinkinsights` • `session.options.enableLinkinsights` For more information, see the *List of System Properties* topic in the *VeloCloud Orchestrator Deployment and Monitoring Guide*.
Multi-scope access for VeloBrain	This feature is available only on managed Orchestrators. Operators can access the VeloBrain feature on the Orchestrator by setting the values of the following two system properties: • `sessions.options.enableVeloAI` • `vco.system.configuration.data.veloAiNginxRedirection` **Note:** After setting the values, Operators must refresh the **System Properties** page to view the VeloBrain icon. Operators can enable the VeloBrain feature for Partners and grant them the privilege to manage it for their Customers. For more information, see Configure a Partner. Operators can also directly enable this feature for specific Customers.
Time-Based One Time Passcode (TOTP)	The TOTP mechanism for Two Factor Authentication replaces the current SMS mechanism. Activating TOTP prevents users from switching back to the SMS option. For more information, see the following topics: • Authentication • Time-Based One Time Passcode (TOTP)

Release Notes

For information on all the **Resolved** and **Known** issues for 7.0.0, see *VeloCloud SD-WAN 7.0.0 Release Notes*.

Chapter 2

About VeloCloud SD-WAN Operator Guide

The VeloCloud SD-WAN™ Operator Guide provides information about VeloCloud Edge Cloud Orchestrator, including configuring and managing Customers and Partners who use the Orchestrator.

Intended Audience

Use this for Operators and Service Providers who are familiar with Networking and SD-WAN operations.

Review the list of topics for the user journey as an Operator super user:

1. Installing SD-WAN Orchestrator
2. Configuring SD-WAN Orchestrator Disaster Recovery
3. Uploading Software Images
4. Configuring System Properties
5. Configuring Operator Users
6. Configuring Operator Profiles
7. Configuring Customers
8. Configuring Partners
9. Configuring User Agreements
10. Managing Edge Licensing
11. Provisioning Edges
12. Configuring Gateways and Gateway Pools
13. Configuring Profiles
14. Monitoring Customers
15. Monitoring and Troubleshooting Gateways
16. Troubleshooting SD-WAN Orchestrator

Chapter 3

Overview of VeloCloud Edge Cloud Orchestrator

VeloCloud Edge Cloud Orchestrator provides centralized, enterprise-wide installation, configuration, and real time monitoring, in addition to orchestrating the data flow through the cloud network.

The Orchestrator provides a web-based user interface to configure and manage the following:

- Customers
- Partners
- Operator Users
- Gateways and Gateway Pools
- Orchestrator Authentication Modes

Chapter 4

Supported Browsers

The Orchestrator supports the following browsers:

Table 2: Supported Browsers

Browsers Qualified	Browser Version
Google Chrome	77 – 79.0.3945.130
Mozilla Firefox	69.0.2- 72.0.2
Microsoft Edge	42.17134.1.0- 44.18362.449.0
Apple Safari	12.1.2-13.0.3

Note: For the best experience, VeloCloud recommends Google Chrome or Mozilla Firefox.

Note: Starting from VeloCloud SD-WAN version 4.0.0, the support for Internet Explorer has been deprecated.

Chapter 5

Log into the Orchestrator Using SSO for an Operator User

Discusses logging into Orchestrator using Single Sign On (SSO) as an Operator user.

- Ensure to configure SSO authentication in Orchestrator.
- Ensure to set up users, roles, and OIDC application for the SSO in your preferred IDPs.

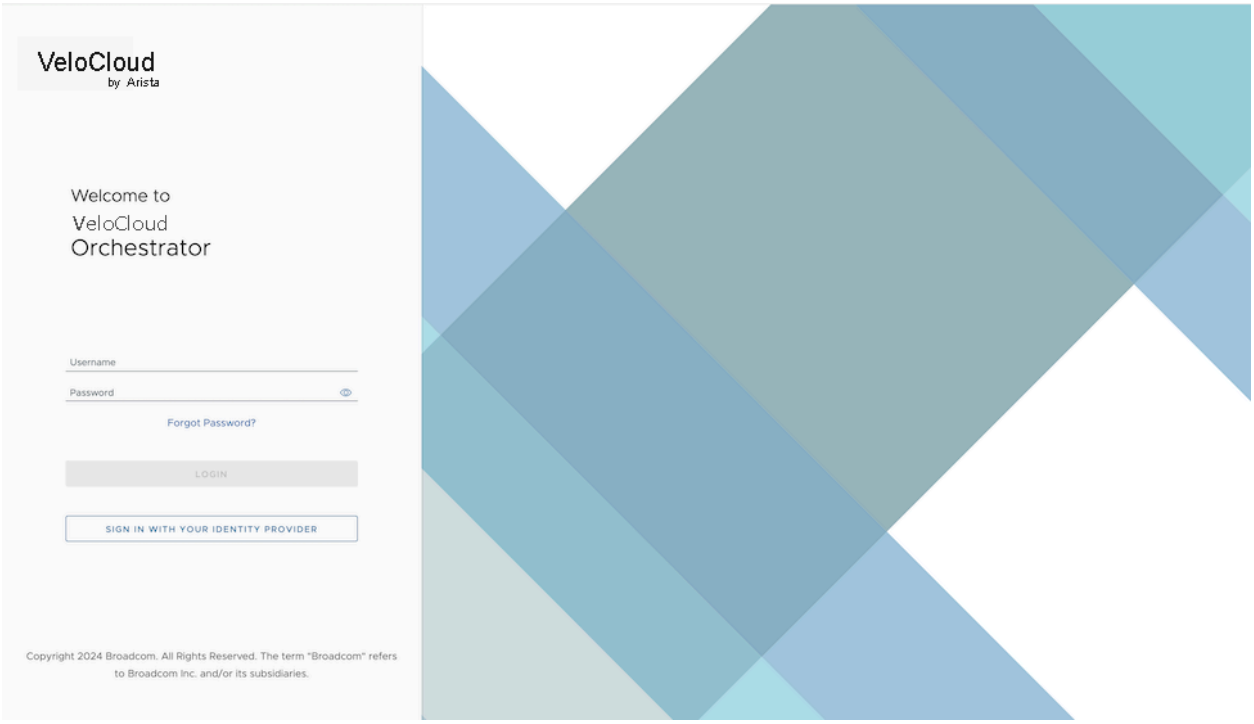
  For additional information, see Authentication.

> **Note:** If other authentication mechanisms fail, there must always be a native Operator Superuser as a system fallback.

To login into Orchestrator using the SSO as an Operator user:

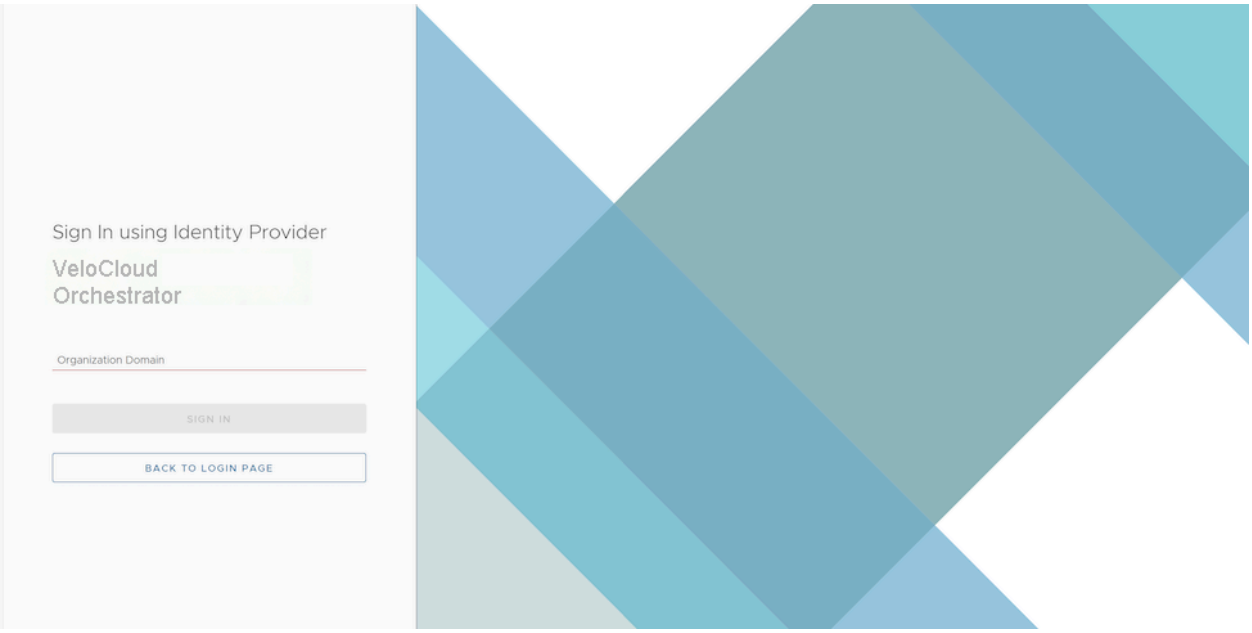
1. In a Web browser, launch the Orchestrator application as an Operator user.

   Figure 5-1: Log into VeloCloud Orchestrator



2. Select **Sign In With Your Identity Provider**.

Figure 5-2: Sign In Using Identity Provider



3. In **Organization Domain**, enter the domain name used for the SSO configuration and select **Sign In**. The IdP configured for the SSO authenticates the user and redirects the user to the configured Orchestrator URL.

> **Note:** Once the users log in to the Orchestrator using the SSO, they cannot log in again as native users.

Next Steps

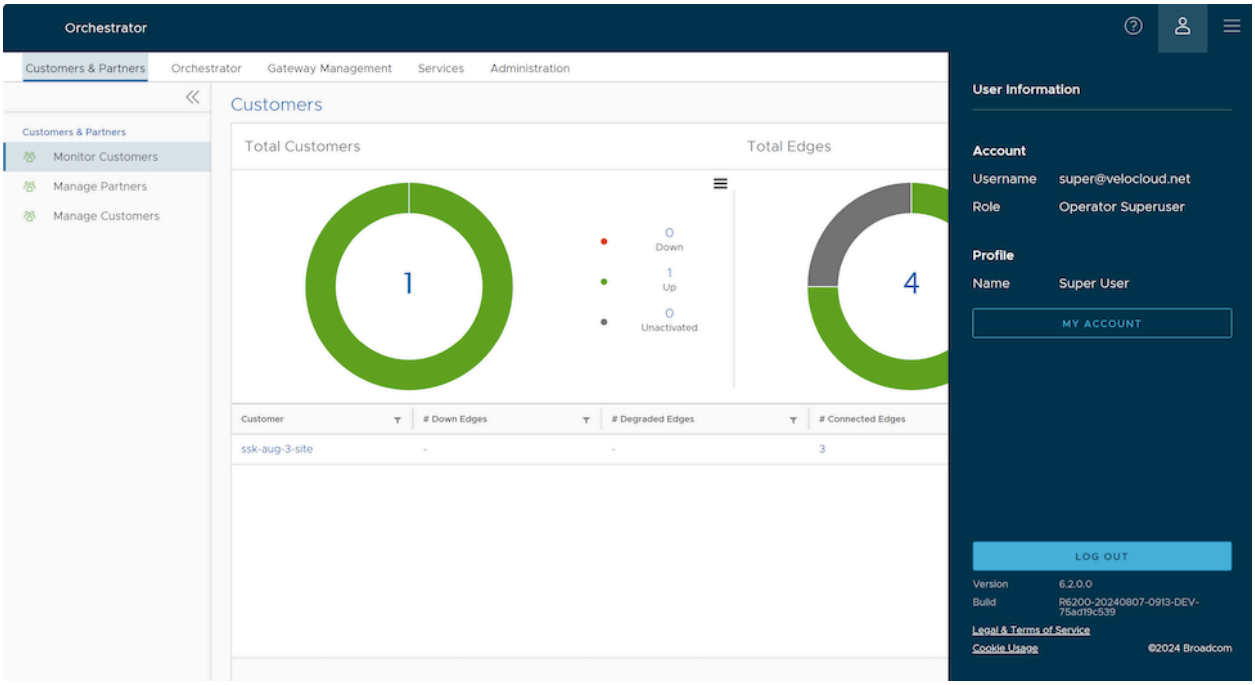
- Manage Customers and Partner
- Manage Operators
- Configure User Account details
- Manage Gateway pools and Gateways
- Manage Software and Firmware images

Additionally, from the **Orchestrator** page, users can access the following features from the **Global Navigation** bar:

- The user selects the **User** icon to access the **My Account** page. The **My Account** page allows users to configure basic user information, SSH keys, and API tokens. Users can also view the current user

role, associated privileges, and additional information such as version number, build number, legal and terms information, and cookie usage. For additional information, see Configure User Account details.

Figure 5-3: Monitor Customers Dashboard



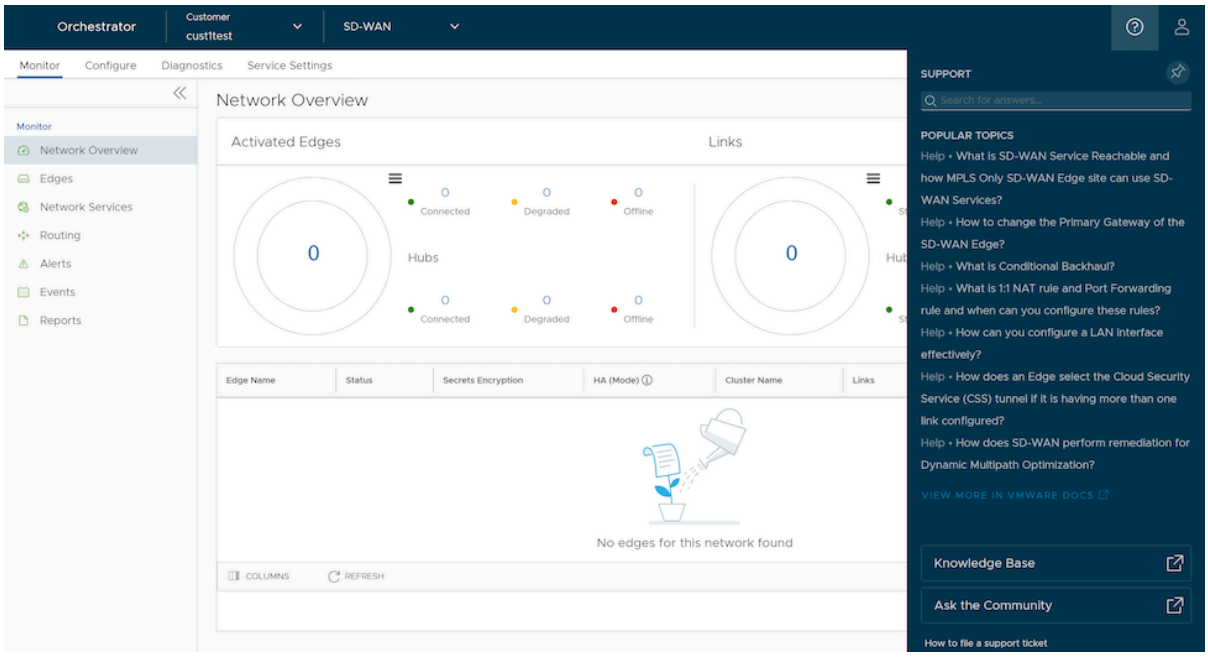
- Starting with the 5.4.0 release, Orchestrator supports the **In-product Contextual Help Panel**, with context-sensitive user assistance, as well as for the Operator and Partner levels. In the Global Navigation bar, select the **Question Mark** icon to access the Support panel.

  The **Support** panel allows users across all levels to access helpful and important information such as Question-Based Lists (QBLs), Knowledge base links, Ask the Community link, how to file a support ticket, and other related documentation from within the Orchestrator page. This makes it easier for the user to learn Orchestrator without navigating to another site for guidance or contact the Support Team.

  Note: By default, the Support Panel does not have availability to all Customers. Users can activate this feature for a Customer by navigating to the **Global Settings** > **Customer**

Configuration > **Additional Configuration** > **Global** > **Feature Access** page. For additional information, see Configure Customers.

Figure 5-4: Monitor Network Overview



Chapter 6

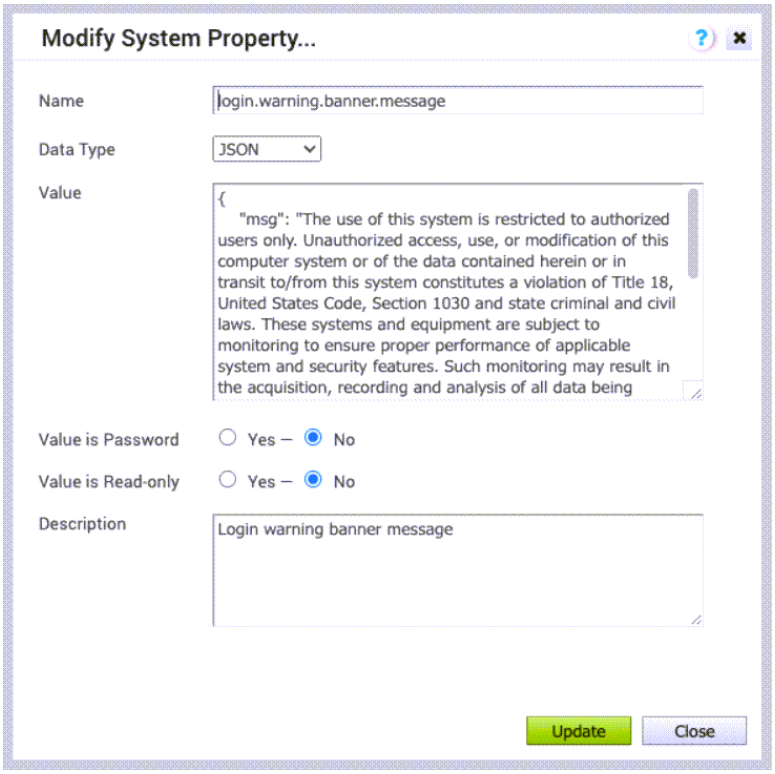
Configure the Advisory Notice and Consent Warning Message for Orchestrator

An Operator user can configure and display a Security Administrator-specified advisory notice and consent warning message regarding the use of Orchestrator for Operators, Partners, and Enterprises.

To configure the consent warning message:

1. In the **Operator** portal, go to **System Properties**.
2. Search and locate the `login.warning.banner.message` system property.
3. Select the system property, and then select **Actions** > **Modify System Property**. The **Modify System Property …** page displays:

   Figure 6-1: Modify System Property



4. Ensure that the **Data Type** field is set to **JSON**.
5. In the **Value** text area, the default value is as follows:

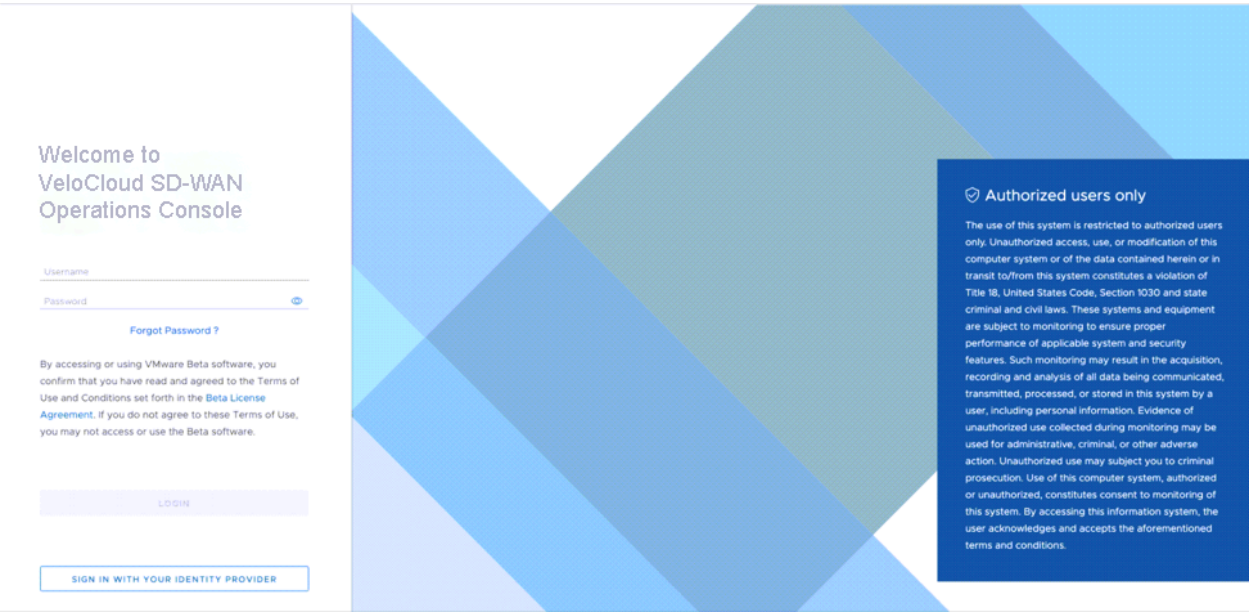
```
{
  "msg": ""
}
```

   In the **msg** variable, type the required warning message between " ".
6. Ensure the **Value is Password** and **Value is Read-only** fields are set to **No**.

7. Select **Update**.

   The warning message displays in the Orchestrator prior to user login for Operator, Partner, and Enterprise.

Figure 6-2: VeloCloud SD-WAN Operations Console Displaying Warning Message



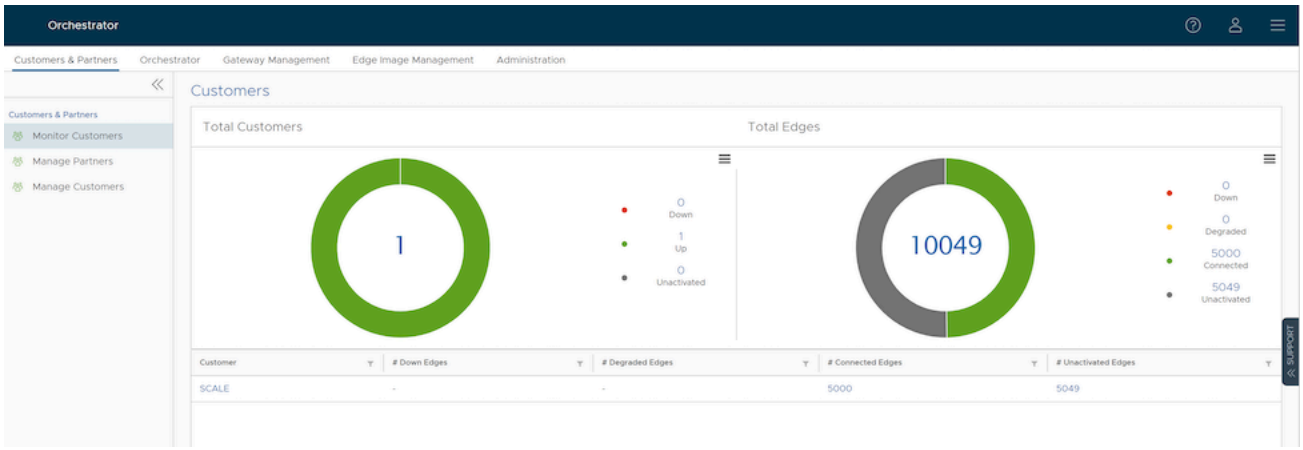
Chapter 7

Monitor Customers

As an Operator user, monitor the status of Customers and the Edges connected to the system.

Log in to the VeloCloud Edge Cloud Orchestrator as an Operator user. In the SD-WAN service of the Operator portal, select **Customers & Partners** > **Monitor Customers**.

Figure 7-1: Monitor Customers Dashboard



The **Customers** page displays the following details:

Total Customers

- Customers managed by the Operator.
- Number of Customers that are UP, DOWN, and UNACTIVATED. Select the number to view the corresponding Customer details in the bottom panel.
- In the bottom panel, select the Customer name to navigate to the **Enterprise** portal, where the user can view and configure other settings corresponding to the selected customer. For additional information, see the *VeloCloud SD-WAN Administration Guide*.

Total Edges

- Edges associated with the Customers.
- Number of Edges that are DOWN, DEGRADED, CONNECTED, and UNACTIVATED. Select the number to view the corresponding details of the Edges in the bottom panel.
- In the bottom panel, place the mouse pointer on the Down Arrow displayed next to the number of Edges, to view the details of each Edge. Select the Edge name link to navigate to the **Enterprise Monitoring** portal, where the user can view more details for the selected Edge. For additional information, see the *VeloCloud SD-WAN Administration Guide*.

Note: Orchestrator does not provide an option for auto refresh. The user must refresh the window manually to view the current data.

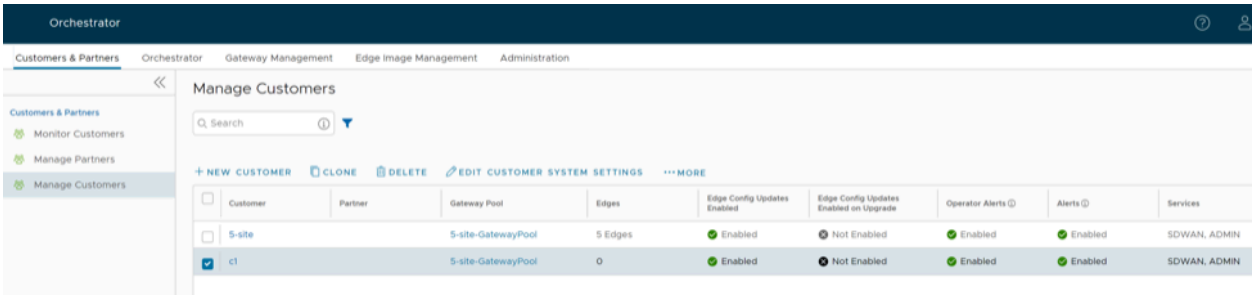
Chapter 8

Manage Customers

The **Manage Customers** option allows users to create new Customers, configure the Customer capabilities, clone the existing configuration, and to configure other Customer settings.

1. In the **Operator** portal, navigate to **Customers & Partners** > **Manage Customers**.

   Figure 8-1: Manage Customers



2. Perform the following actions:

   Table 3: Manage Customers - Options and Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
New Customer	Select this option to add a new Customer. For more information, see Create New Customer
Clone	Clones the selected Customer's existing configurations. The user can select any of the additional clone attributes. For more information, see Clone a Customer.
Delete	Deletes the selected Customers. Enter the number of selected Customers in the pop-up window, and then select **Delete**. **Note:** Ensure the user removes all Edges associated with the selected Customer before deleting the Customer.
Edit Customer System Settings	Allows the user to edit the customer's system settings. For more information, see the *Enterprise Settings* section in the *VeloCloud SD-WAN Administration Guide*.
Stage to Bastion	Select to stage a Customer to the Bastion Orchestrator.

Note: Stage to Bastion and **Unstage from Bastion** options are available only when the Bastion Orchestrator feature is activated using the `session.options.enableBastionOrchestrator` system property.

For additional information, see *Bastion Orchestrator Configuration Guide*.

3. Select **More** to perform the following actions:

Table 4: Additional Option Descriptions

Option	Description
Unstage from Bastion	Removes a Customer from the Bastion Orchestrator.
Edit Customer Edge Management	Allows to edit the Edge Management feature for the selected Customers.
Transfer to Partner	Assigns the selected Customer to a Partner. The user can select an existing Partner from the drop-down list.
Release from Partner	Releases the selected Customer from the Partner.
Send Support Email	Sends customer support messages to the selected Customer.
Assign Operator Profile	Adds an Operator Profile for the selected Customers.  **Note:** This option is available only for an Enterprise with the Edge Image Management feature activated.
Update Edge Image Management	Activates or deactivates the Edge Image Management feature for the selected Customers.
Update Operator Alerts	Activates or deactivates the Operator alerts for the selected Customers.
Update Customer Alerts	Activates or deactivates the Customer alerts for the selected Customers.
Rebalance Gateways	Rebalances the Gateways of Edges associated with the selected Customer
Export All Customers	Exports the details of all the Customers in the Operator portal to a CSV file. The default separator used is a comma (,).
Export Customers Edge Inventory	Exports the inventory details for all Edges associated with all Customers to a CSV file. The default separator used is a comma (,).

4. Following are the other options available in the **Manage Customers** area:

Table 5: Manage Customers Option Descriptions

Option	Description
Columns	Select this option and select the checkbox to view the required columns.
Refresh	Select this option to refresh the page.

To configure a customer, see Configure Customers.

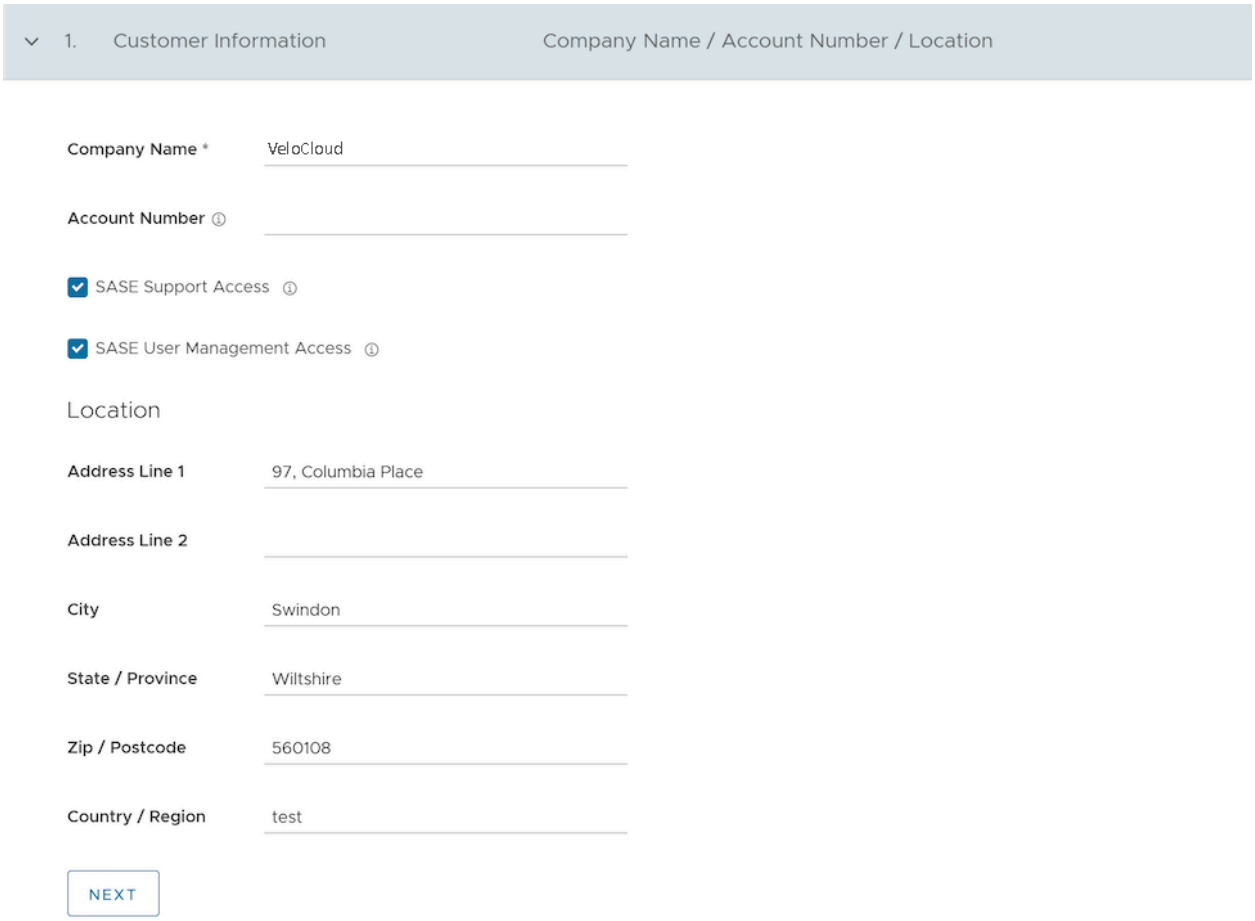
8.1 Create a New Customer

In the **Operator** portal, users can create Customers and configure the Customer settings. Only Operator Super Users and Operator Standard Admins can create a new Customer. As an Operator Super User, the user can temporarily deactivate creation of new Customers by setting the system property `session.options.disableCreateEnterprise` to **True**. The user can select this option when Orchestrator exceeds the usage capacity.

1. In the **Operator** portal, go to **Customers & Partners** > **Manage Customers**, and then select **New Customer**. The **New Customer** page displays:

Customer Information:

Figure 8-2: Configure Customer Information



2. Enter the details in the following fields and select **Next**.

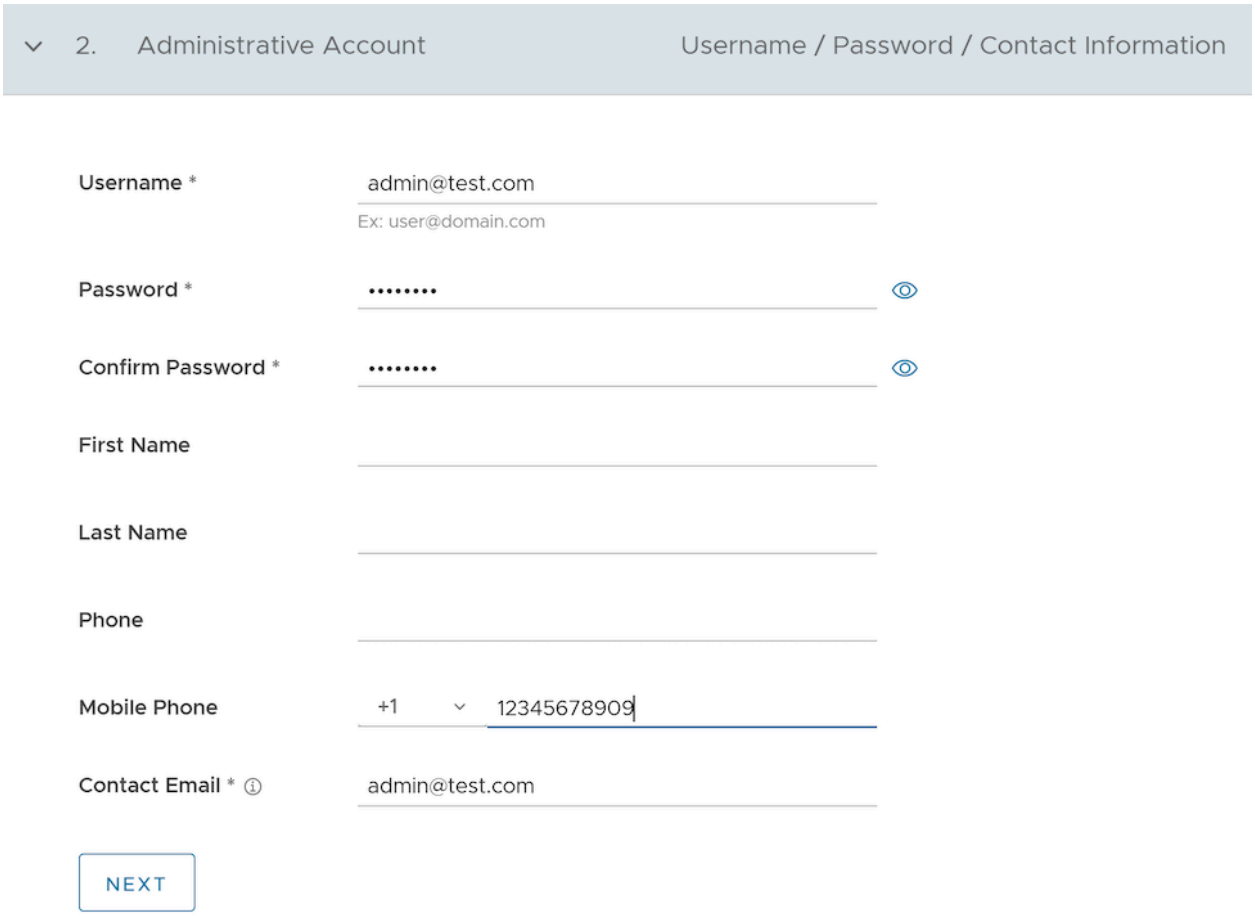
Note: Entering all mandatory details activates the **Next** button.

Table 6: New Customer option Description

Option	Description
Company Name	Enter company name.
Account Number	Enter a unique identifier for the Customer.
SASE Support Access	This check box is selected by default, and grants access to the Arista Support to view, configure, and troubleshoot the Edges connected to the Customer. For security reasons, the Support cannot access or view the user identifiable information.
SASE User Management Access	Select the check box to allow the Arista Support to assist in User Management. The User Management includes options to create users, reset password, and configure other settings. In this case, the Support has access to user identifiable information.
Location	Enter relevant address details in the respective fields.

3. The **Administrative Account** displays:

Figure 8-3: Configure an Administrative Account



4. Enter the details in the following fields and select **Next**.

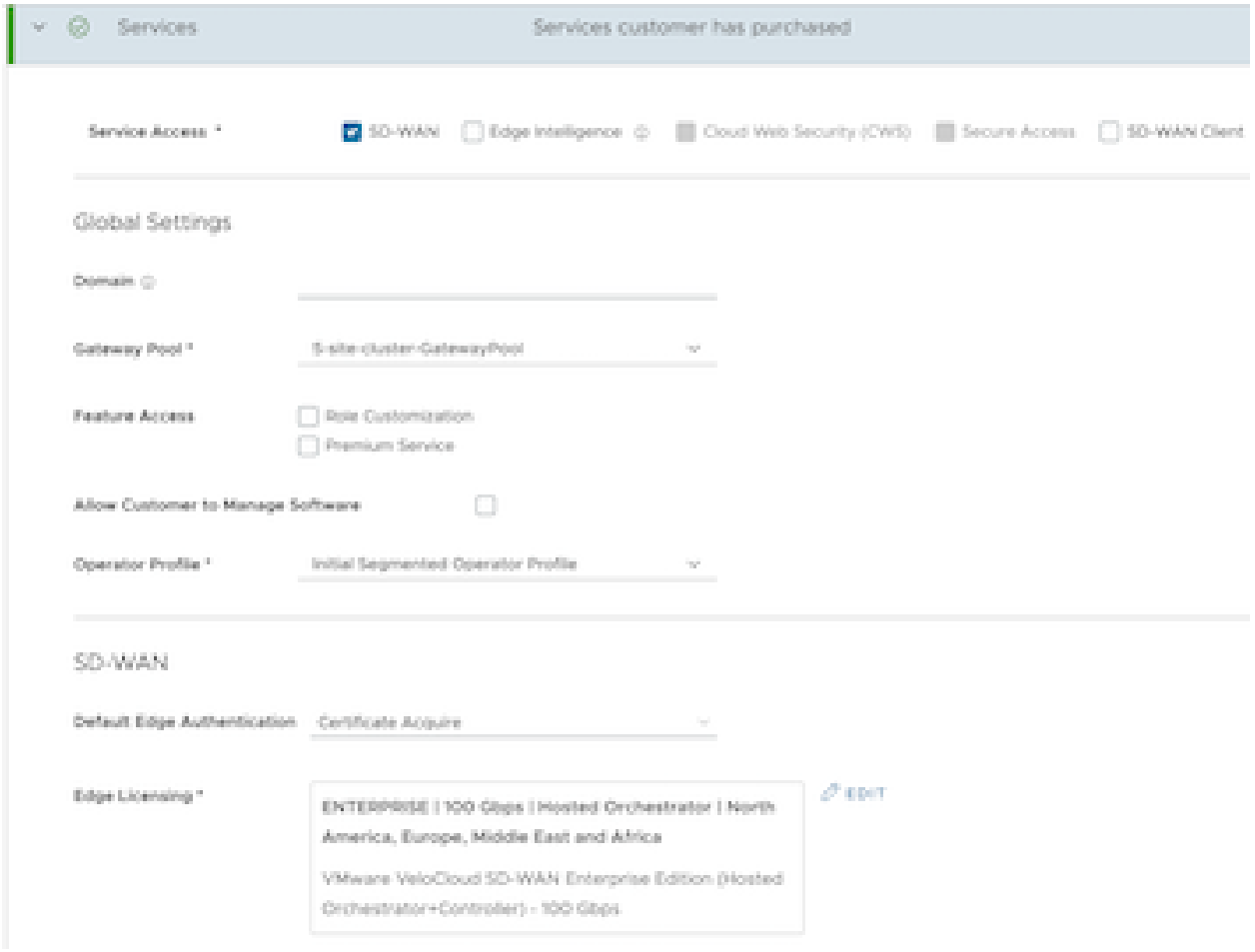
> **Note:** Entering all mandatory details activates the **Next** button.

Table 7: Administrative Account Option Description

Option	Description
Username	Enter the username in the `user@domain.com` format.
Password	Enter a password for the Administrator. **Note:** Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Confirm Password	Re-enter the password.
First Name	Enter the first name.
Last Name	Enter the last name.
Phone	Enter a valid phone number.
Mobile Phone	Enter a valid mobile number.
Contact Email	Enter the email address. The alerts on service status are sent to this email address.

5. Selecting **Next** displays the **Services** section:

Figure 8-4: Configure Services



6. Configure the following **Global Settings**:

Table 8: Global Settings Option Descriptions

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator.
Gateway Pool	Select an existing Gateway pool from the drop-down list. For additional information, see Manage Gateway Pools.
Feature Access	Select either **Role Customization** or **Premium Service**, or both the check boxes.
Allow Customer to Manage Software	Select the checkbox to allow an Enterprise Super User to manage the software images available for the Enterprise. Once selected, the **Software Image** field is displayed. Select **Add** and in the **Select Software/Firmware Images** pop-up window, select and assign the software/firmware images from the available list for the Enterprise. Select **Done** to add the selected images to the **Software Image** list. **Note:** Remove an assigned image from an Enterprise, only if the image is not currently used by any Edge within the Enterprise. For additional information, see Platform and Modem Firmware and Factory Images and Software Images.
Operator Profile	Select an Operator profile to be associated with the Customer from the available drop-down list. This field is not available if **Allow Customer to Manage Software** is selected. For additional information on Operator profiles, see Manage Operator Profiles.

7. **Service Access**: This option is available above the **Global Settings** section. The user can choose which services the Customer can access, along with the roles and permissions available for each service.

   Note: This option is available only when the system property `session.options.enableServiceLicenses` is set as **True**.

8. **SD-WAN**- When the user selects this service, the following options are available:

Table 9: Service Access Option Description

Option	Description
Default Edge Authentication	Choose the default option to authenticate the Edges associated with the Customer, from the drop-down list. • **Certificate Deactivated**: Edge uses a pre-shared key mode of authentication. • **Certificate Acquire**: This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the Orchestrator and for establishment of VCMP tunnels. **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**. • **Certificate Required**: Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property `edge.certificate.renewal.window`.
Edge Licensing	Select **Add** and in the **Select Edge Licenses** pop-up window, select and assign the Edge licenses from the available list for the Enterprise. **Note:** Multiple Edges support these license types. Provide customers with all license types to ensure they match their edition and region. For additional information, see Edge Licensing.
Feature Access	Select the **Stateful Firewall** checkbox to override the Stateful Firewall settings activated on the Enterprise Edge.

9. After entering all the details, select the **Add Customer** button.

   If the user wants to add another customer, Select **Add another Customer** before **Add Customer** to add multiple customers. The new customer name appears on the **Customers** page. The user can select the Customer name to navigate to the Enterprise portal and add configurations to the Customer.

   For additional information, see Configure Customers.

8.2 Clone a Customer

The user can clone the configurations from an existing customer and create a new customer with the cloned settings.

Only Operator Super users and MSP Super users can clone a customer.

By default, the following configurations are cloned from the selected customer:

- Enterprise configuration profiles
- Enterprise network services and objects like:
  - DNS services
  - Private network names
  - Network Segments

- Customer capabilities
- Edge authentication scheme
- Address groups and Port groups

Note: Distributed Cost Calculation does not copy to the cloned Enterprise.

The user cannot clone an Enterprise if it consists of the following:

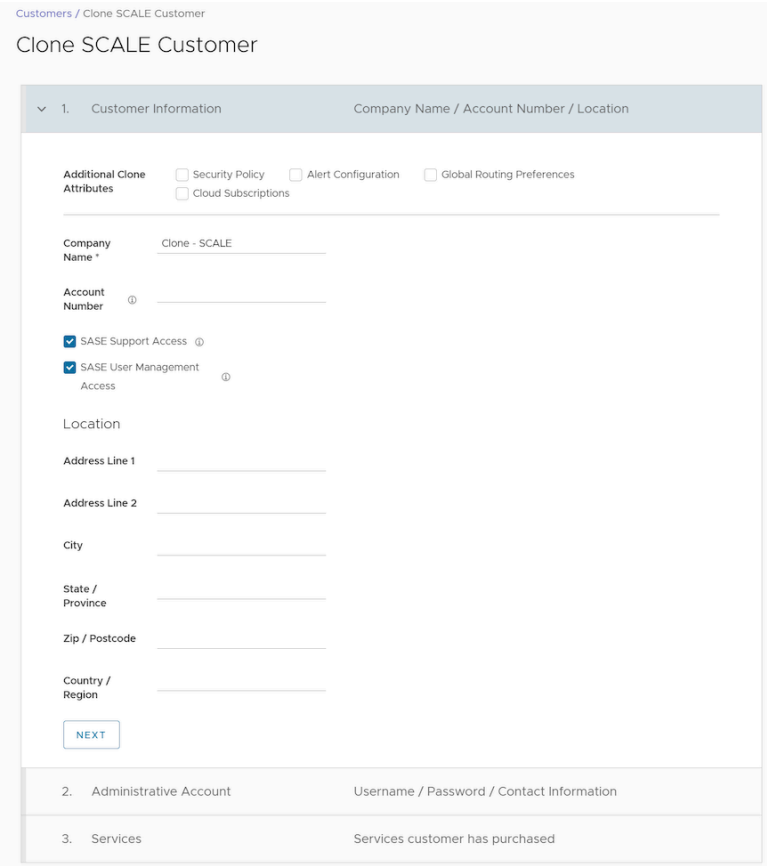
- Profile with Edge references, such as hubs and clusters.
- Profile containing Partner Gateway References
- Cloud Security Service enabled
- Non SD-WAN Destinations
- VNF or VNF licenses
- Authentication services
- NetFlow objects, like collectors or filters

Log in to the VeloCloud Edge Cloud Orchestrator as an Operator user. Navigate to **Customers & Partners** > **Manage Customers**.

1. On the **Customers** page, select the customer the user wants to clone, and then select **Clone**.

2. The **Clone Customer** page appears.

Figure 8-5: Clone a Customer



3. Configure the **Customer Information**, **Administrative Account** details, and **Services**. For additional information, see Create New Customer.
4. Select **Add Customer**.

   The new customer name appears on the **Customers** page. The customer now uses the cloned settings. The user can select the customer name to navigate to the Enterprise portal and add or modify the configurations.

   For additional information about customer configurations and settings, see Configure Customers.

8.3 Configure Customers

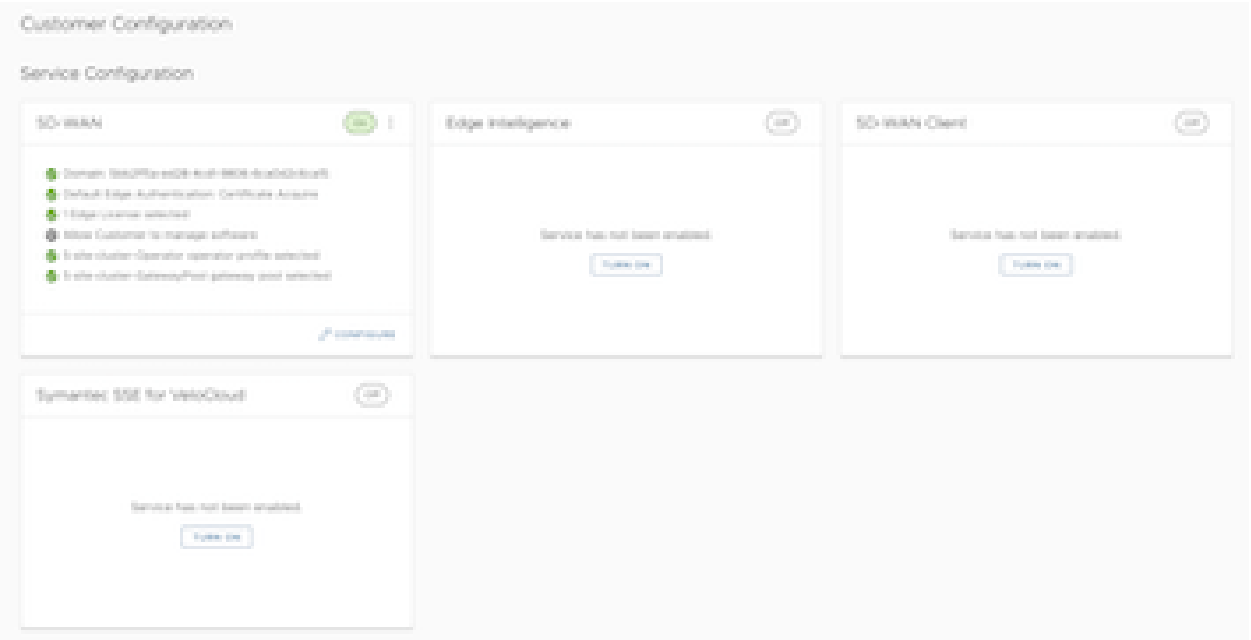
After creating a Customer, configure the feature options and settings that the Customer can access. As an Operator, choose the settings that the Customer can modify.

When you create a new Customer, you are redirected to the **Customer Configuration** page, where you can configure the Customer settings. Users can also navigate to the **Customer Configuration** page directly from the **Operator** portal by following the below steps:

1. On the **Monitoring and Configuration Options** page, select a **Customer**, and from the top header, select **SD-WAN** > **Global Settings**.

2. From the left menu, select **Customer Configuration** to display the page:

Figure 8-6: Customer Configuration



3. The **Service Configuration** section includes the **SD-WAN** service. Select **Turn On** to activate the service. Select the vertical ellipsis in the top right corner of the tile to turn off or configure the service. You can also select the **Configure** option, located at the bottom right corner of the tile, to configure the respective service. The tile displays the configuration summary.

> **Note:** When you select the **Turn off** option, a pop-up window appears asking for your confirmation. Select the checkbox and select **Turn Off Service**.

Configure SD-WAN

Select the **Configure** option to display the **SD-WAN Configuration** section. Configure the settings, and then select **Update**.

Figure 8-7: SD-WAN Configuration

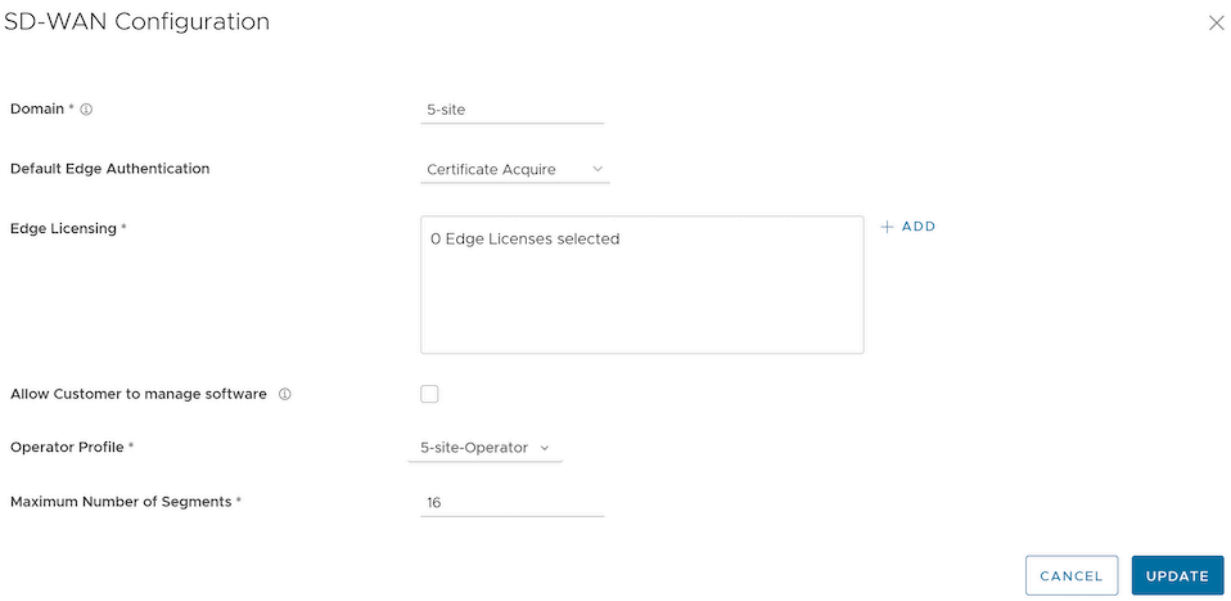


Table 10: SD-WAN Configuration - Options and Descriptions

Option	Description
Domain	Enter the domain name to be used to activate Single Sign On (SSO) authentication for the Orchestrator.
Default Edge Authentication	Choose the default option with authenticate the Edges associated to the Customer from the drop-down menu. • **Certificate Deactivated:** Edge uses a preshared key authentication mode. • **Certificate Acquire:** This option is selected by default and instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication with the Orchestrator and for establishing VCMP tunnels. **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**. • **Certificate Required:** Edge uses the PKI certificate. Operators can change the certificate renewal time window for Edges using the system property `edge.certificate.renewal.window`.
Edge Licensing	The existing Edge Licenses are displayed. Select **Add** to add or remove the licenses. **Note:** License types are used across multiple Edges. It is recommended to provide your Customers with access to all types of licenses to match their edition and region. For additional information, see Edge Licensing.
Allow Customer to Manage Software	Select the checkbox if you want to allow an Enterprise Superuser to manage the software images available for the Enterprise. For additional information, see the topic *Edge Image Management* in the *VeloCloud SD-WAN Administration Guide*.
Operator Profile	Select an Operator profile to be associated with the Customer from the available drop-down menu. This field is not available if **Allow Customer to Manage Software** is selected. For additional information on Operator profiles, see Manage Operator Profiles.
Maximum Number of Segments	Enter the maximum number of segments that can be configured. The valid range is 1 to 16. The default value is **16**.

Configure Additional Settings

1. Following are the additional configuration settings available on the **Customer Configuration** page:

Table 11: Additional Configuration - Options and Descriptions

Option	Description
Global	
User Agreement Display	Select either of the following from the drop-down menu: • Inherit • Override to Hide • Override to Show **Note:** This field is available only when the system property `session.options.enableUserAgreements` is set to **True**.
Feature Access	Provides access to the selected features. Select one or more checkboxes from the below list to activate these features for the Customer: • **Enterprise Auth**- By default, only the Operator can activate or deactivate two-factor authentication for an Enterprise. When you select this checkbox, the Enterprise Admins can configure two-factor authentication. This option also controls Single Sign-On (SSO) activation and deactivation. • **Enable Premium Service**- This option is selected by default. Premium Service refers to the On-Demand Remediation feature, a core part of SD-WAN Dynamic Multipath Optimization (DMPO). All traffic that traverses a VeloCloud Gateway uses DMPO. When Premium Service is selected, the Gateway uses Forward Error Correction (FEC) for customer traffic impacted by high levels of WAN link jitter or loss, and which cannot be steered to a better quality WAN link. When Premium Service is not selected, traffic still traverses the VeloCloud Gateway and benefits from other components of DMPO like Continuous Monitoring, Dynamic Application Steering, and Secure Traffic Transmission. However, traffic impacted by high levels of WAN link jitter or loss does not benefit from error correction by the Gateway. For additional information, see the topic *Dynamic Multipath Optimization (DMPO)* in the *VeloCloud SD-WAN Administration Guide*. • **Role Customization**- Allows an Enterprise Super user to customize the role privileges for other Enterprise users. • **Route Backtracking**- Allows the device to choose the best route in the order of prefix length. • **In-product Contextual Help Panel**- Provides access to the 'In Product Help' panel integrated within the Orchestrator. This feature is deactivated by default. An Operator must activate this option for the Enterprise Customers. • **Enable Firewall Logging to Orchestrator**- By default, Edges cannot send their Firewall logs to the Orchestrator. Select this checkbox to allow an Edge to send the Firewall logs to the Orchestrator. • **Customizable QoE**- Allows the Customer to configure the minimum and maximum latency threshold values for Voice, Video, and Transactional application categories of an Edge. • **Enable Classic Orchestrator UI**- Allows the Customer to switch from the Angular Orchestrator UI to the Classic Orchestrator UI. This option is available only when the system property `session.options.enableClassicOrchestrator` is set to **True**.

Option	Description
Delegate Management To Customer	Allows the Customer to modify the settings of the selected property. Following two properties are always visible to the Customers: • **Enable CoS Mapping**- Allows the configuration of CoS mapping while configuring a business policy. • **Enable Service Rate Limiting**- Allows for rate limiting services in a business policy.
Gateway Pool	
Current Gateway Pool	Displays the current Gateway pool associated with the selected Customer. If required, you can choose a different Gateway pool available in the drop-down menu and select **Save Changes**.
Gateways in this Pool	Displays the Gateway details in the current pool.
Partner Hand Off	Activating the **Gateway Pool** option displays the **Configure Hand Off** section. If the Gateways in the Gateway pool have been assigned the Partner Gateway role, you can hand off the Gateways to Partners. For details, see *Configure Partner Gateway Handoff to Production Orchestrator Configure Partner Handoff*.
Security Policy	
Hash	By default, there is no authentication algorithm configured for the VPN header, as AES-GCM is an authenticated encryption algorithm. When you select the **Turn off GCM** checkbox, you can select one of the following as the authentication algorithm for the VPN header from the drop-down menu: • **SHA 1** • **SHA 256** • **SHA 384** • **SHA 512**
Encryption	Select either **AES 128** or **AES 256** as the AES algorithm's key size to encrypt data. The default encryption algorithm mode is **AES 128**. **Note:** The AES configuration affects only phase 2 tunnels.
DH Group	Select the Diffie-Hellman (DH) Group algorithm to be used when exchanging a pre-shared key. The DH Group sets the strength of the algorithm in bits. The supported DH Groups are 2, 5, 14, 15, 16, 19, 20, and 21. **Note:** • DH Groups 19, 20, and 21 are available starting from Release 5.2.0. • It is recommended to use DH Group 14, which is the default value.
PFS	Select the Perfect Forward Secrecy (PFS) level for additional security. The supported PFS Groups are 2, 5, 14, 15, 16, 19, 20, and 21. PFS Groups 19, 20, and 21 are available starting in Release 5.2.0. By default, PFS is deactivated.
Turn off GCM	Select this checkbox to activate **Hash** and select an authentication algorithm for the VPN header.
IPSec SA Lifetime Time(min)	Time when Internet Security Protocol (IPSec) rekeying is initiated for Edges. The minimum IPsec lifetime is 3 minutes and the maximum IPsec lifetime is 480 minutes. The default value is 480 minutes. **Note:** It is not recommended to configure a low lifetime value for IPsec (less than 10 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.

Option	Description
IKE SA Lifetime(min)	Time when Internet Key Exchange (IKE) rekeying is initiated for Edges. The minimum IKE lifetime is 10 minutes and maximum IKE lifetime is 1440 minutes. The default value is 1440 minutes. **Note:** It is not recommended to configure low lifetime values for IKE (less than 30 minutes), as it can cause traffic interruption in some deployments due to rekeys. The low lifetime values are for debugging purposes only.
Secure Default Route Override	Select the checkbox so that the destination of traffic matching a secure default route (either Static Route or BGP Route) from a Partner Gateway can be overridden using Business Policy.

Edge Network Function Virtualization- Allows to activate NFV on the Edges and allows Customers to deploy third party VNFs on service ready Edge platforms. Currently, the service ready Edge platform models are 520v and 840. As an Operator User, when you activate the **Edge NFV**, Customers can configure and deploy VNFs and VNF licenses from their network services.

Edge NFV	Select this option to activate the ability to deploy VNFs on Edges. After deploying one or more VNFs on Edges, you cannot deactivate this option.
Security VNFs	Select the relevant checkboxes to deploy the corresponding security VNFs on Edges. For additional information, see the topic *Security VNFs* in the *VeloCloud SD-WAN Administration Guide*.

SD-WAN Settings

OFC Cost Calculation	Select the required checkbox: • **Distributed Cost Calculation**: Select this checkbox to delegate route cost calculation to Edges/Gateways. **Note:** This option is available only for the Edges/Gateways with version 3.4.0 and later. After activating **Distributed Cost Calculation**, it is recommended to refresh the routes by navigating to **Configure** > **Overlay Flow Control** in the **SD-WAN** service of the Enterprise portal. For additional information, see Configure Distributed Cost Calculation. • **Use NSD Policy**- Select this checkbox to use NSD policy for route cost calculation to Edges/Gateways. **Note:** This option is available only for the Edges/Gateways with version 4.2.0 and later.
Multiple-DSCP tags per Flow Path Calculation	This feature is used when the original user traffic is encapsulated in another tunnel (GRE/IPsec), and the DSCP labels are saved in the new IP header. The feature activates path calculation for a single flow (same source/destination) with multiple DSCP tags and offers path differentiations based on the DSCP values in the flow. Select the **Include DSCP value as part of flow lookup** checkbox to include DSCP values as part of flow look-up and path calculation. For additional information, see Configure Path Calculation with Multiple DSCP Labels per Flow. **Note:** This field is available only when the system property `session.options.enableFlowParametersConfig` is set to **True**.

Feature Access

Stateful Firewall	Select the **Stateful Firewall** checkbox to override the Stateful Firewall settings activated on the Enterprise Edge.

Option	Description
Enhanced Firewall Services	Select the **Enhanced Firewall Services** checkbox to activate the Enhanced Firewall Services using the Firewall functionality in VeloCloud Orchestrator. **Note:** For Enhanced Firewall Services (EFS) to work, ensure the Edge version is upgraded to 5.2.0.0. **Note:** Deselecting this option only deactivates the EFS feature in the UI. To deactivate the EFS feature for an existing customer, you must first deactivate the EFS feature in the SD-WAN service of the Enterprise portal by navigating to **Configure** > **Profiles/Edges** > **Firewall** > **Firewall Feature Control** > **Enhanced Security** and then by clearing this checkbox in **Global Settings**. For additional information about configuring the various Enhanced Security Services and associating them with a Firewall rule, see the topic *Configure Enhanced Security Services* in the *VeloCloud SD-WAN Administration Guide*.

2. Select **Save Changes**.

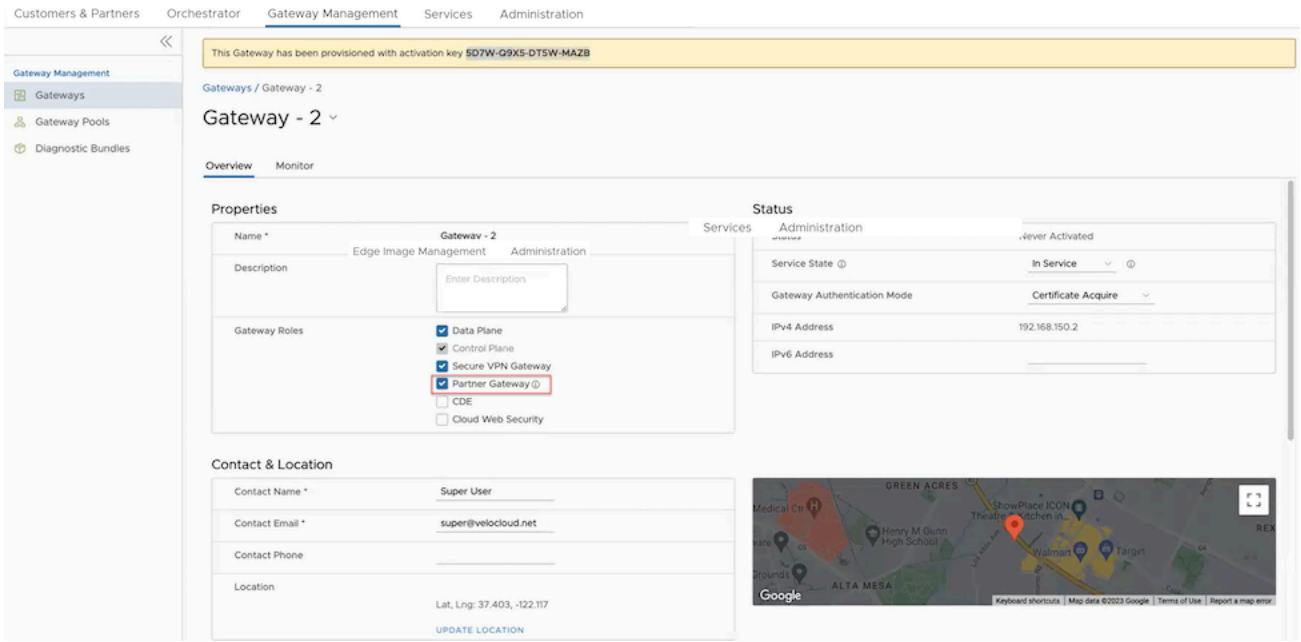
Note: When you modify the **Security Policy** settings, the changes may cause interruptions to the current services. In addition, these settings may reduce overall throughput and increase the time required for VCMP tunnel setup, which may impact branch to branch dynamic tunnel setup times and recovery from Edge failure in a cluster.

8.3.1 Configure a Handoff Operator

You can configure a Gateway to hand off to Partners. The Gateway acts as a Partner Gateway, enabling you to configure the Handoff Interface, Static Routes, BGP, and other settings.

Ensure that the Gateway to hand off is assigned the Partner Gateway Role. In the Orchestrator portal, Operator or Partner, select **Gateways** and select the link to an existing Gateway. In the **Properties** section of the selected **Gateway Overview** page, you can enable the **Partner Gateway** role.

Figure 8-8: Manage Gateways



To configure the handoff settings, perform the following steps:

1. Log in to the Orchestrator as an Operator user.
2. Navigate to **Customers and Partners** > **Manage Customers**.
3. In the **Manage Customers** window, select the link of the desired customer.
4. Go to **Global Settings** > **Customer Configuration**.
5. In the **Customer Configuration** window, scroll down to **Additional Configuration** and expand the **Gateway Pool** area.
6. Enable **Partner Hand Off**.
7. In the **Configure Hand Off** area, configure the following fields:

Figure 8-9: Configure Hand Off

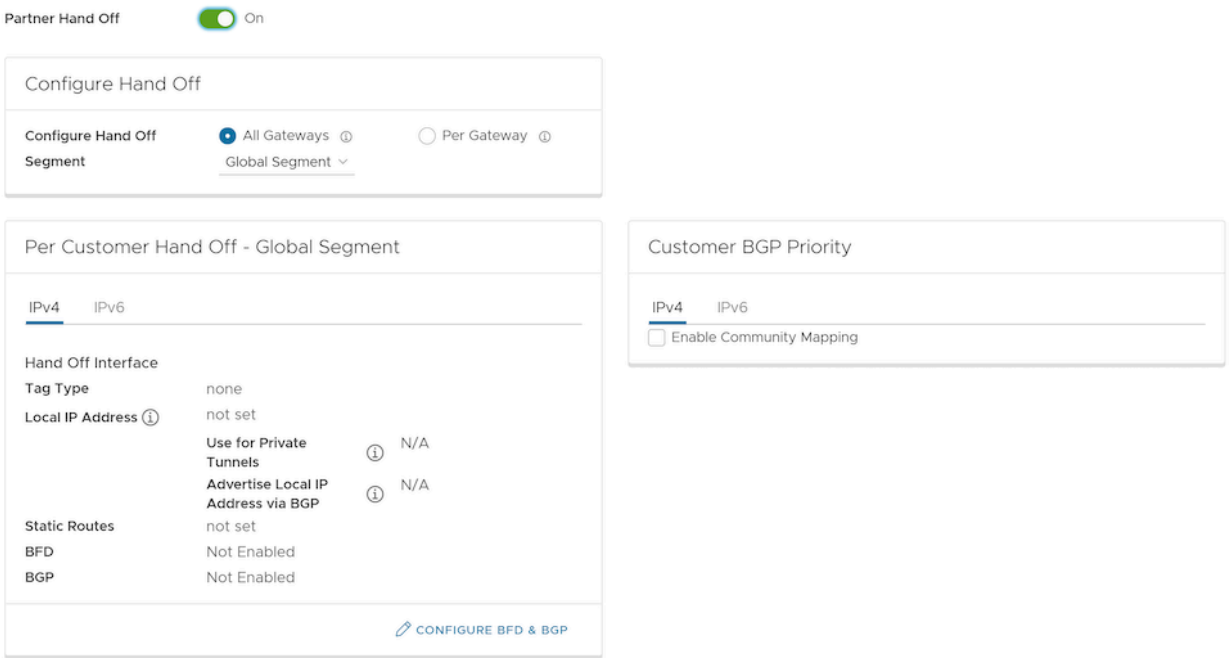
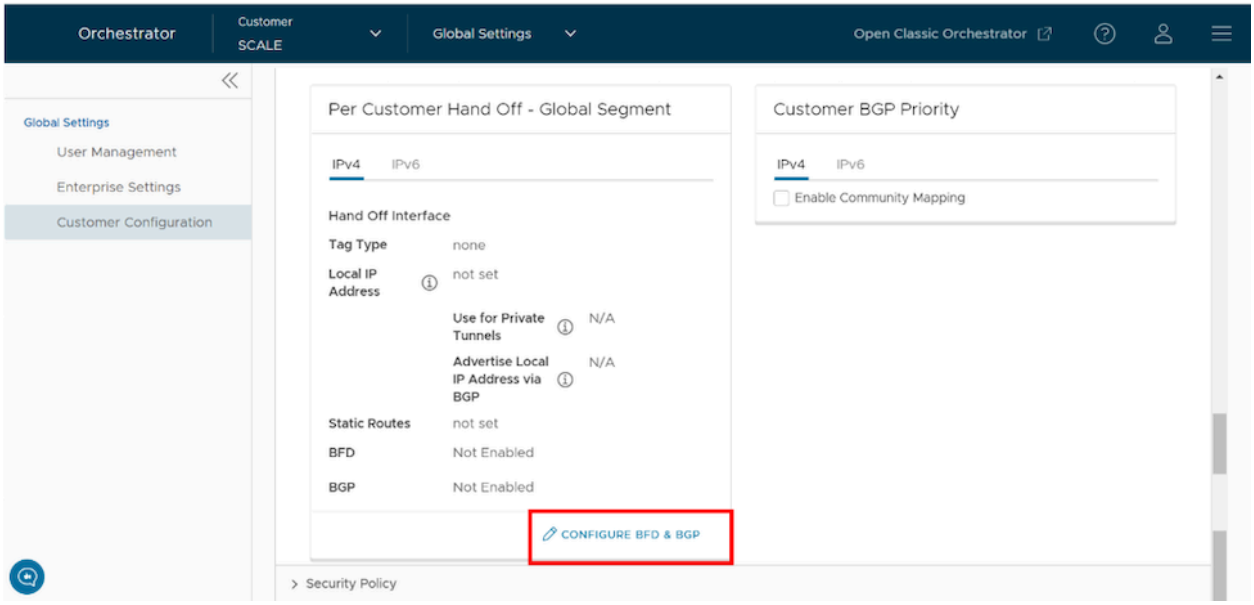


Table 12: Hands Off Option Descriptions

Option	Description
Configure Hand Off	By default, the hand off configuration is applied to all the Gateways. If you want to configure a specific Gateway, choose **Per Gateway**, and then select the Gateway from the drop-down list.
Segment	By default, the **Global Segment** is selected, which means that the hand off configuration is applied to all the segments. If you want to configure a specific segment, select the segment from the drop-down menu.
Hand Off Interface	This section displays the values that are configured on the **Configure BGP and BFD** page.
Customer BGP Priority	Select the check box and configure the **Community Mapping** details.

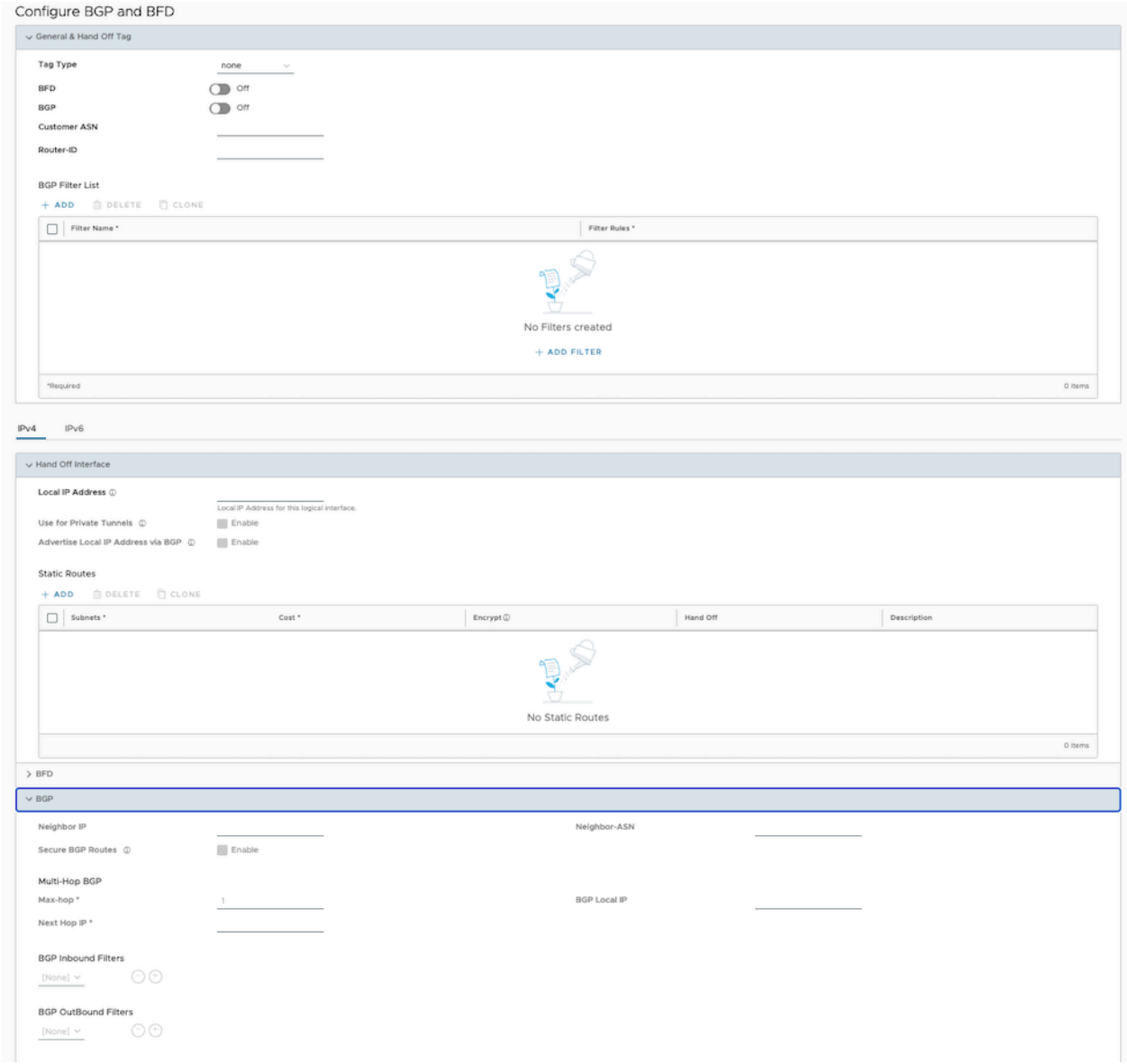
8. At the bottom of the **Per Customer Hand Off – Global Segment** area, select the **Configure BFD and BGP** link.

Figure 8-10: Per Customer Handoff with Global Segment



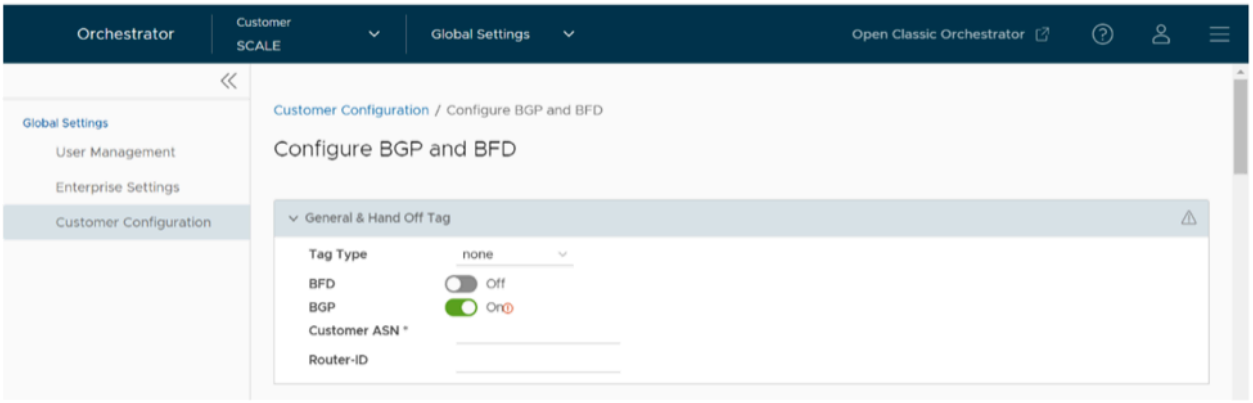
9. The **Configure BGP and BFD** screen displays:

Figure 8-11: Configure BGP and BFD



10. Open the **General & Hand Off Tag** section and turn the **BGP** option to the **On** position.

Figure 8-12: Enable BGP



11. Scroll down to the **BGP** section and select the arrow to display the **BGP** section.
12. Configure the following fields:

Table 13: BGP Option Descriptions

Option	Description
Hand Off Tag	
Tag Type	Choose the tag type, which is the encapsulation, in which the Gateway hands off customer traffic to the Router. The following are the types of tags available: • **None**- Untagged. Choose this during a single-tenant handoff or a handoff towards shared services VRF. • **802.1Q**- Single VLAN tag • **802.1ad / QinQ(0x8100) / QinQ(0x9100)**- Dual VLAN tag
Customer ASN	Enter the Customer Autonomous System Number.
Hand Off Interface: You can configure the following settings for IPv4 and IPv6.	
Local IP Address	Enter the Local IP address for the logical Hand Off interface.
Use for Private Tunnels	Select the check box so that private WAN links connect to the private IP address of the Partner Gateway. If private WAN connectivity is activated on a Gateway, the Orchestrator audits to ensure that the local IP address is unique for each Gateway within an Enterprise.
Advertise Local IP Address via BGP	Select the check box to automatically advertise the private WAN IP of the Partner Gateway through BGP. The connectivity is provided using the existing Local IP address.
Static Routes: You can add, delete, or clone a static route.	
Subnets	Enter the IP address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply weighting on the routes. The range is from 0 to 255.
Encrypt	Select the check box to encrypt the traffic between Edge and Gateway.
Hand off	Select the hand off type as either **VLAN** or **NAT**.
Description	Enter a descriptive text for the static route. This field is optional.
BFD: Turn the toggle button to On to activate this section.	
Peer Address	Enter the IP address of the remote peer to initiate a BFD session.
Detect Multiplier	Enter the detection time multiplier. The remote transmission interval is multiplied by this value to determine the detection timer for connection loss. The range is from 3 to 50.
Receive Interval	Enter the minimum time interval, in milliseconds, at which the system can receive the control packets from the BFD peer. The range is from 300 to 60000 milliseconds.
Local Address	Enter a locally configured IP address for the peer listener. This address is used to send the packets.
Transmit Interval	Enter the minimum time interval, in milliseconds, at which the system can send the control packets from the BFD peer. The range is from 300 to 60000 milliseconds.
BGP: Turn the toggle button to On to activate this section.	
Neighbor IP	Enter the IP address of the configured BGP neighbor network.
Secure BGP Routes	Select the check box to allow encryption for data-forwarding over BGP routes.
Max-hop	Enter the number of maximum hops to allow multi-hop for the BGP peers. The Max-hop range is 1 to 255, with and default value of 1.  **Note:** This field is available only for eBGP neighbors when the local ASN and the neighboring ASN are different.

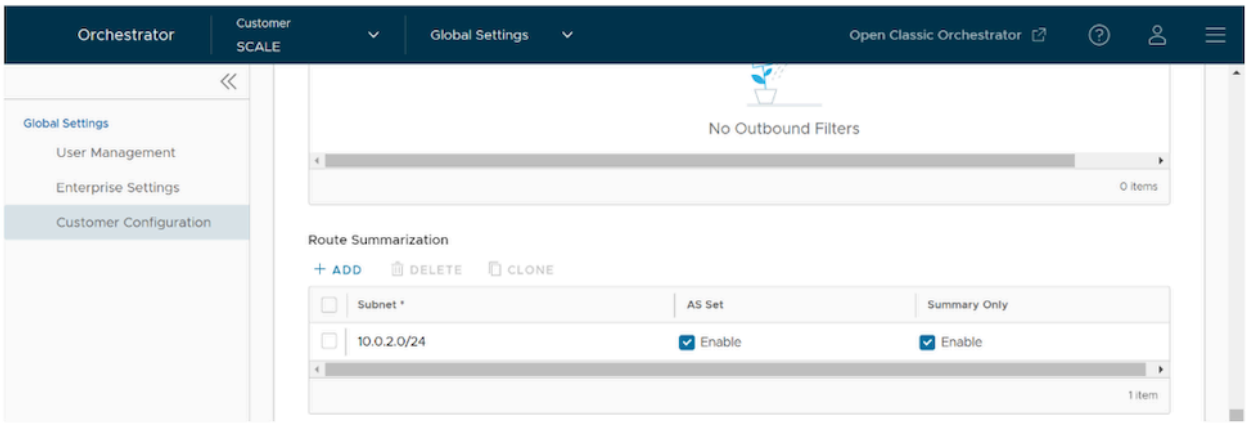
Option	Description
Next Hop IP	Enter the next-hop IP address to be used by BGP to reach the multi-hop BGP peer. **Note:** This option is available only for multi-hop eBGP with a Max-hop count greater than 1.
Neighbor-ASN	Enter the Autonomous System Number of the Neighbor network.
BGP Local IP	Local IP address is the equivalent of a loopback IP address. Enter an IP address that the BGP neighborships can use as the source IP address for the outgoing BGP packets. **Note:** The BGP Local IP address must be from a different subnet than the handoff IP address. If you do not enter any value, the IP address of the **Hand Off Interface** is used as the source IP address.
BGP Filter List	Configure BGP filters.
BGP Inbound Filters	Assign a filter to inbound.
BGP Outbound Filters	Assign a filter to outbound.
BGP Optional Settings	
BFD	Select the check box to subscribe to the BFD session.
Router-ID	Enter the Router ID to identify the BGP Router.
Keep Alive	Enter the BGP Keep Alive time in seconds. The default timer is 60 seconds.
Hold Timers	Enter the BGP Hold time in seconds. The default timer is 180 seconds.
Turn off AS-PATH Carry Over	Select the check box to turn off AS-PATH carry over, which influences the outbound AS-PATH to make the L3-routers prefer a path towards a PE. If you select this option, ensure to tune your network to avoid routing loops. It is recommended not to select this check box.
MD5 Auth	Select the check box to activate BGP MD5 authentication. This option is used in a legacy or federal network and serves as a security guard for BGP peering.
MD5 Password	Enter a password for MD5 authentication. **Note:** Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.

Configuring Route Summarization

Route Summarization is new for the 5.2 release. For an overview, use case, and black hole routing details for Route Summarization, see the *Route Summarization* section in the *VeloCloud SD-WAN Administration Guide*. For Route Summarization configuration details, follow the steps below:

1. Navigate to the **Route Summarization** area in the **BGP** section.

Figure 8-13: Configure Route Summarization



2. Configure the **Route Summarization** fields:

Table 14: Route Summarization Option Descriptions

Option	Description
+Add	Select +Add to add a new row in the **Route Summarization** area. **Note:** To add additional rows to configure Route Summarization, select **+Add**. To Clone or delete a route summarization, use the appropriate buttons, located next to **+Add**.
Subnet column	Under the **Subnet** column, enter the IP subnet.
AS Set column	Generate AS set path information from the summarized routes (while advertising the summarized route to the peer). Under the **AS Set** column, select the **Yes** check box if applicable.
Summary Only column	Under the **Summary Only** column, select the **Yes** check box to allow only the summarized route to be sent.

3. Select **Update** to save the settings.

8.3.2 Configure Distributed Cost Calculation

By default, the Orchestrator actively learns the dynamic routes. VeloCloud SD-WAN Edges and Gateways rely on the Orchestrator to calculate initial route preferences and return them to the Edge and Gateway. The Distributed Cost Calculation feature enables you to distribute the route cost calculation to the Edges and Gateways. Only an Operator user can configure Customer settings, including Distributed Cost Calculation.

Ensure the following before you activate the Distributed Cost Calculation feature.

- All the Edges and Gateways must use software version 3.4.0 or later.
- The software image associated with the Operator Profile must use version 3.4.0 or later.

Note: If experiencing an issue with Orchestrator based route calculation, enable **Distributed Cost Calculation**.

This default method of using Orchestrator in both dynamic route calculation and the distribution of those routes to Edges and Gateways has the following drawbacks:

- If the Orchestrator is under a high load, the route convergence time is significantly high, for example, as much as 40 seconds for 2000+ routes, as the Orchestrator takes that time to calculate the preference for all the synchronized routes and returns those preferences to the Edges and Gateways.
- Using the Orchestrator for route calculation means that new dynamic routes learned while the Orchestrator was unreachable do not advertise until the Orchestrator becomes reachable again.

When a customer enterprise uses Distributed Cost Calculation, the Orchestrator is no longer actively involved in the route preference calculation and instead routes are properly inserted in order by the Edge and Gateway instantly upon learning them and then convey these preferences to the Orchestrator.

When you choose to enable Distributed Cost Calculation for the Edges and Gateways, the feature provides the following benefits:

- Minimizes the impact on route learning when an Orchestrator is unreachable.
- Route convergence time is reduced from minutes to seconds in large networks with thousands of dynamic routes.
- Network delays are significantly reduced.
- Provides instantaneous Data Plane convergence.
- Supports enhanced re-ordering and pinning of routes on the Overlay Flow Control.
- Provides an option to refresh routes on the **Overlay Flow Control** page. Whenever the Overlay Flow Control policy changes, the Refresh Routes option applies the changes to the existing routes immediately, without requiring a restart of the Edge or Gateway.

Enabling Distributed Cost Calculation has the following impacts on the Customer Enterprise network:

- All local dynamic routes are refreshed, and their preference and advertisement actions are updated. This updated information is advertised to the Gateway and Orchestrator, and eventually across the Enterprise. The customer's network needs to completely rebuild the route table, which for most customer deployments will take less than 5 seconds. A large scale customer deployment (like 100,000+ routes) may take up to 2 minutes. During the time the route table is being rebuilt, customer traffic for all sites is impacted.
- Any existing flows using these routes may be affected by the change in the routing entries.

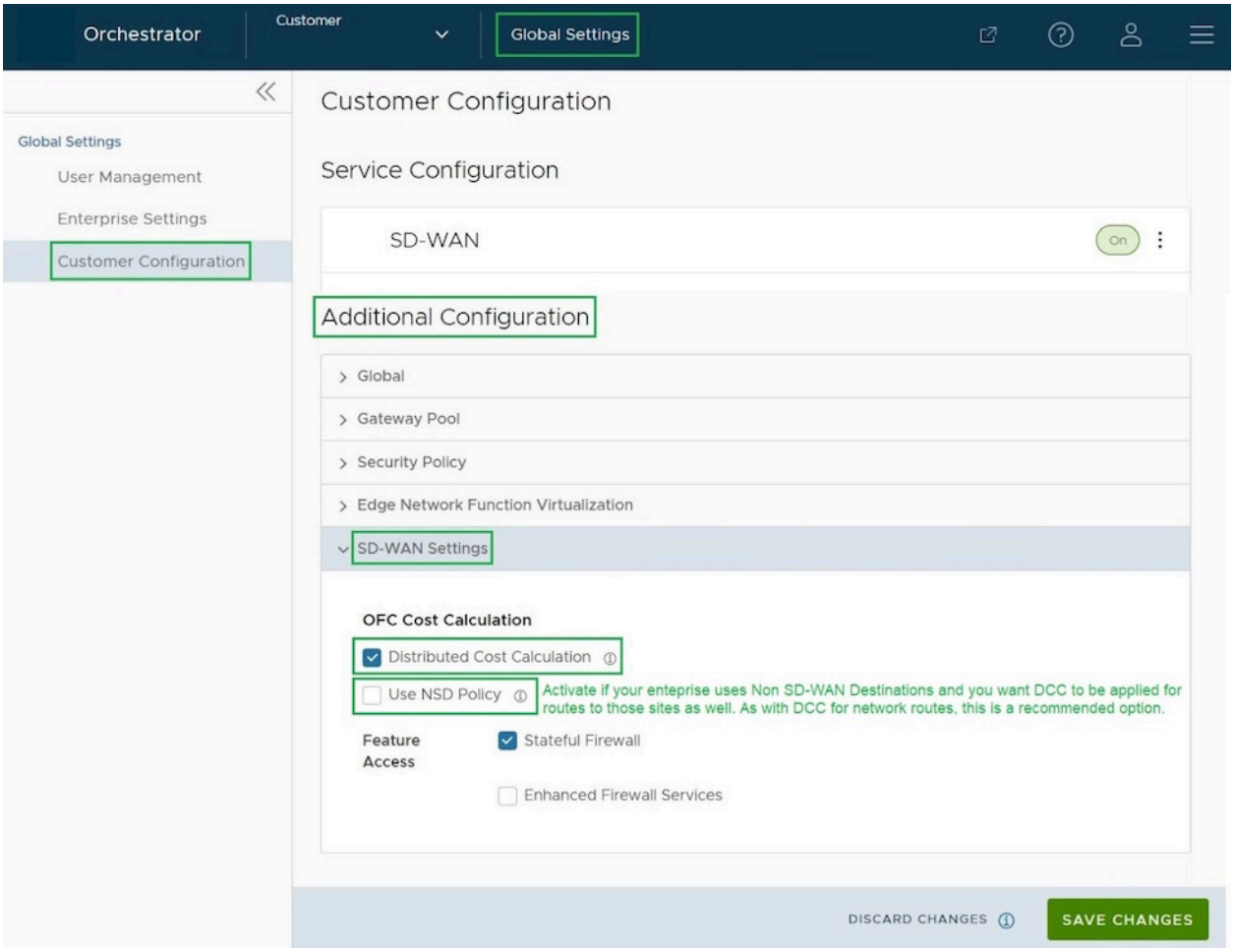
Note: It is recommended to enable Distributed Cost Calculation in a maintenance window to minimize the impact on the Customer Enterprise.

To configure Distributed Cost Calculation for a customer:

1. In the **Operator** portal, navigate to **Manage Customers**.
2. Select a customer, then either select **Edit Customer System Settings** or select the link to the customer.

3. In the **Enterprise** portal, go to **Global Settings** > **Customer Configuration**.

Figure 8-14: Configure Distributed Cost Calculation



4. On the **Customer Configuration** page, navigate to the **Additional Configuration** > **SD-WAN Settings** > **OFC Cost Calculation** section and configure the following:
   - Select the **Distributed Cost Calculation** checkbox to delegate the cost calculation of routes to Edges and Gateways.
   - Select the **Use NSD Policy** checkbox to use the Non SD-WAN Destination policy for route cost calculation of Edges and Gateways. This option is available only for Edges and Gateways running Software version 4.3.0 or later.
5. Select **Save Changes**.

Note: After enabling **Distributed Cost Calculation**, it is recommended to refresh the routes in the **Overlay Flow Control** page in the **SD-WAN** service of the **Enterprise** portal.

Note: When an Enterprise has **Distributed Cost Calculation** activated and a user tries to deactivate the software update on the **Operator Profile** page, then the user must ensure that, in the future, no Edges in the Enterprise are downgraded to software image versions lower than 3.4.0. If one or more Edges in the Enterprise are using software image version below 3.4.0, the Enterprise traffic may take a sub-optimal path. The sub-optimal path will be corrected only when the Edge is upgraded to 3.4.0 or later versions.

The following are some of the scenarios in which the software versions can change, and the user must make sure the Edges are using the software image version 3.4.0 or later:

- Factory Reset- When an Edge is reset to the factory settings, it restores the software version of the Edge to factory image version, which can be below 3.4.0.
- Edge Activation- When an Edge is activated, it may come up with software versions below 3.4.0.

Once **Distributed Cost Calculation** activates, all the dynamic routes are assigned new preferences and advertise action based on the Distributed Cost Calculation. The new information is propagated across the Enterprise Network.

The Orchestrator is no longer actively involved in the route preference calculation. Instead, the routes are properly inserted in order by the Edge, and the Gateway instantly upon learning them, and then these preferences are conveyed to the Orchestrator.

The Overlay Flow Control policy is sent to Edges and Gateways in Control Plane Configuration updates. Edges and Gateways send the routes with computed cost and advertise action to the Orchestrator. Edges and Gateways handle the order of the routes based on the cost and route attributes.

To view a summary of all the routes in your network, select **Configure** > **Overlay Flow Control** in the **SD-WAN** service of the **Enterprise** portal. You can view the routes and advertise action on the **Overlay Flow Control** page. For additional information, see the topic *Overlay Flow Control* in the *VeloCloud SD-WAN Administration Guide*.

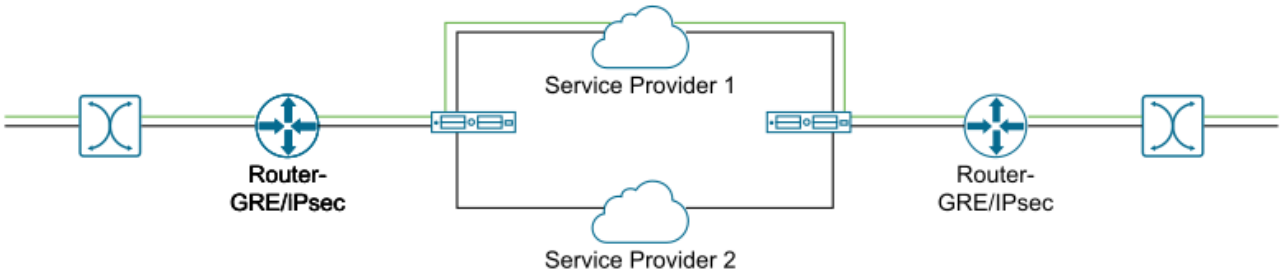
8.3.3 Configure Path Calculation with Multiple DSCP Labels per Flow

An Edge classifies traffic flows based on the first packets in each flow. You can create business policies in an application based on the Differentiated Service Code Point (DSCP) and different DSCP markings to determine flow treatment.

By default, an Edge classifies a flow based on the first few packets received in the flow. Business Policy and QoS marking determine the flow treatment. Once the flow is classified, an entry containing the flow's five-tuple information is created in the flow cache table. Subsequent packets in the flow will use the five-tuple lookup against the flow cache table.

For network topologies with Layer 3 network devices doing encapsulation or encryption before the traffic arrives at the Edge, this creates a challenge for the Edge to forward traffic based on the Business Policy. The traffic from end users is multiplexed into a single flow with the same source and destination IP addresses and protocols by the Layer 3 encapsulation/encryption device, as illustrated in the following image.

Figure 8-15: Traffic Flow



The impact of multiplexing end user flows into a single tunnel creates polarization of the flow forwarding using the five tuples of flow cache table, which results in WAN links not being utilized.

The Path Calculation with Multiple DSCP Labels per Flow allows the DSCP value to be included, along with the five tuples, in the flow cache table lookup. Use the path calculation with multiple DSCP tags when the original user traffic is encapsulated in another tunnel, like GRE or IPsec, and DSCP labels are preserved in the new IP header. This option enables path calculation for a single flow with multiple DSCP labels that share the same source and destination IP addresses. It provides path differentiation based on the DSCP labels in the flow.

When you enable the **Multiple-DSCP tags per Flow Path Calculation**, the Edges can differentiate the traffic flows based on the DSCP marked labels.

To enable Multiple-DSCP tags per Flow Path Calculation:

1. In the **Operator** portal, select **Orchestrator** > **System Properties**.
2. Select **New**.
3. In the **New System Property** window, create a system property with the following parameters:
   - **Name:** `session.options.enableFlowParametersConfig`
   - **Data Type:** *Boolean*
   - **Value:** *True*
4. Select **Save Changes**.
5. In the **Operator** portal, navigate to **Global Settings** > **Customer Configuration** > .
6. On the **Customer Configuration** page, go to the additional configuration settings section, and then under **SD-WAN** settings, select the **Include DSCP value as part of flow lookup** checkbox for **Multiple-DSCP tags per Flow Path Calculation**.

   Note: This option is available only when the system property `session.options.enableFlowParametersConfig` is set to **`True`**.

7. Select **Save Changes**.
8. In the Edges, different flows are created based on different DSCP labels.

   Note: When you select **Include DSCP value as part of flow lookup**, the inter-operability with previous versions is undefined.

   While configuring the business policy for an Edge, you can choose to match a DSCP label for an application. For additional information, see the topic *Configure Business Policy Rule* in the *VeloCloud SD-WAN Administration Guide*.

   When traffic arrives at the Edge, if the traffic flow matches the selected application and DSCP tag, then the corresponding action is performed.

   You can create additional business policies with different DSCP labels to match different traffic flows and apply different treatments for those flows. For additional information on business policies, see the *VeloCloud SD-WAN Administration Guide.*

   Limitations

- The path calculation with multiple DSCP labels per Flow is not applicable for the Gateways. You can enable this option only for Edge-to-Edge tunnels, where Edge-to-Edge can be any of the following:
  - Edge-to-Edge through Hub
  - Spoke-to-Hub
  - Dynamic Branch-to-Branch

  You can use this option for On-Premise deployment, where the Gateway is used only for control plane functionality and not for data plane traffic.
- The path calculation with multiple DSCP labels per Flow is intended only for GRE or IPSec traffic. The direct Internet traffic does not carry multiple DSCP labels within a single flow.
- After you enable the path calculation option, when the traffic flow consists of packets with the same five-tuple information but different DSCP markings, LAN side NAT might not work as expected.

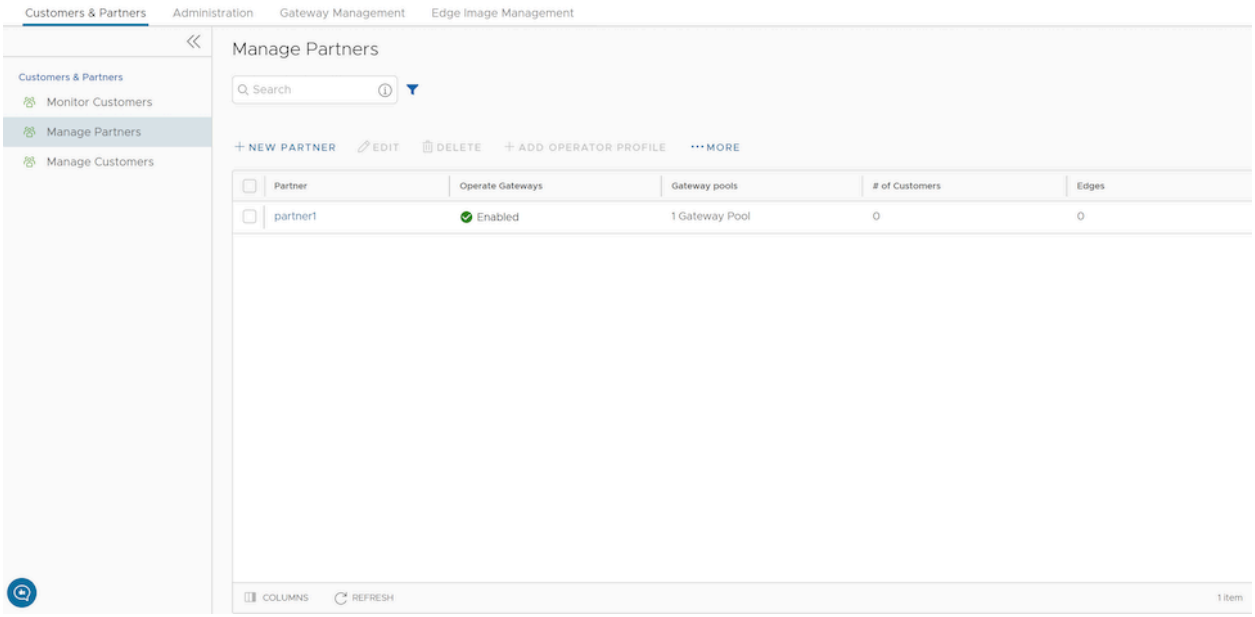
Chapter 9

Manage Partners

The Manage Partners option allows you to create new Partners, who can independently manage a group of Customers.

1. Log in to the VeloCloud Edge Cloud Orchestrator as an Operator user. In the **SD-WAN** service of the **Operator** portal, select **Manage Partners**.

   Figure 9-1: Manage Partners



2. Perform the following actions:

Table 15: Manage partners Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
New Partner	Select this option to add a new Partner. For additional information, see Create New Partner.
Edit	This option takes you to the **Partner Overview** page in the **Partner** portal, where you can edit the **Partner Capabilities**, **Available Software Images**, and **Gateway Pool** of the selected Partner. For additional information, see Configure Partner.
Delete	Deletes the selected Partners. Enter the number of selected Partners in the pop-up window, and then select **Delete**.  **Note:** Ensure that you have removed all Customers associated with the selected Partner before deleting the Partner.
Add Operator Profile	Assigns an Operator profile to the selected Partners, which specifies the network settings managed by Orchestrator. In the **Add Profiles to Selected Partners** pop-up window, select a profile and select the arrow to add it. Select **Save**. For additional information, see Manage Operator Profiles
More	Select this option, then select **Download** to download the list of Partners' profiles in a CSV format.

3. Following are the other options available in the **Manage Partners** area:

Table 16: Manage Partners Additional Option Descriptions

Option	Description
Columns	Select this option, then select the checkboxes to view the required columns.
Refresh	Select this option to refresh the page.

9.1 Create a New Partner

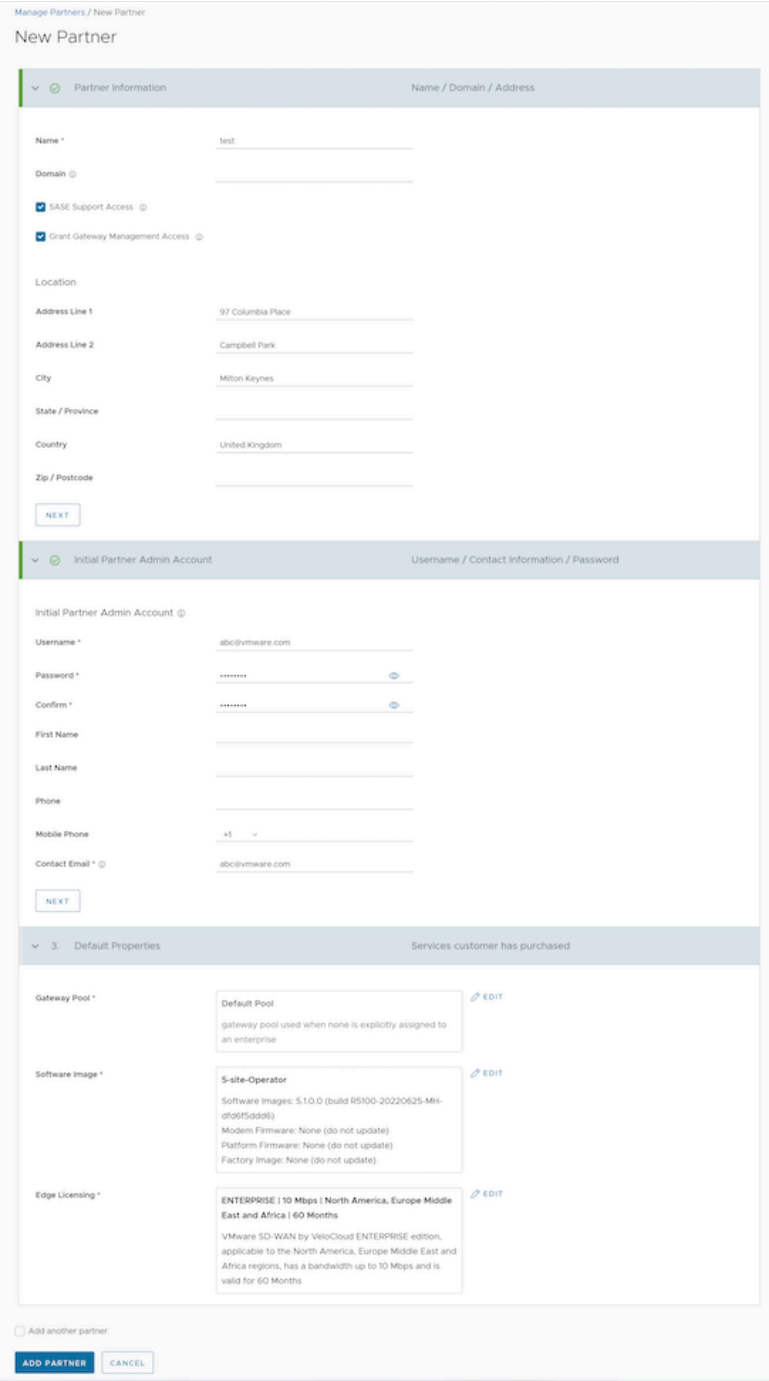
In the **Operator** portal, you can create Partners and configure settings so that Partners can manage a group of Customers.

Only Operator Superusers, Standard Operators, and Business Specialist Operators can create a new Partner.

 **Note:** As an Operator Super User, you can temporarily deactivate creating new partners by setting the system property `session.options.disableCreateEnterpriseProxy` to **True**. You can use this option when Orchestrator exceeds the usage capacity.

1. Log in to the VeloCloud Edge Cloud Orchestrator as an Operator user. In the **Operator** portal, go to **Customers and Partners** > **Manage Partners**, and then select **New Partner**.

   Figure 9-2: Create a New Partner



2. On the **New Partner** page, enter the following details. Select **Next** to go to the next section on the page. The **Next** button is activated only when you enter all the mandatory details in each section.

Table 17: New Partner Option Descriptions

Option	Description
Partner Information	
Name	Enter the Partner name.
Domain	Enter the domain name of the Partner.
SASE Support Access	This option is selected by default and grants access to Arista Support to view, configure, and troubleshoot the settings of the Partner.
Grant Gateway Management Access	Select the checkbox to allow the Partner to create and manage the Gateways.
Location	Enter relevant address details in the respective fields.
Initial Partner Admin Account	
Username	Enter the username in the **user@domain.com** format.
Password	Enter a password for the Partner.  **Note:** Starting from the 4.5 release, the use of the special character "<" in the password is no longer supported. In cases where users have already used "<" in their passwords in previous releases, they must remove it to save any changes on the page.
Confirm	Re-enter the password.
First Name, Last Name, Phone, Mobile Phone	Enter relevant details in the respective fields.
Contact Email	Enter the email address. The alerts on service status are sent to this email address.
Default Properties	
Gateway Pool	Select **Add** to select the Gateway Pool from the available list. After adding the Gateway Pools, select **Edit** to add or remove them. For additional information on Gateway Pools, see Manage Gateway Pools.
Software Image	Select **Add** to select the Software Image from the available list. After adding the Software Image, you can select **Edit** to add or remove the images. For additional information on Software Images, see Firmware and Software Images with New Orchestrator UI.
Edge Licensing	Select **Add** to select the Edge licenses from the available list. After adding the licenses, you can select **Edit** to add or remove the licenses. This option is available only when the value of System Property `session.options.enableEdgeLicensing` is set to True.  **Note:** The license types can be used on multiple VeloCloud Edges. It is recommended to provide the Partners with access to all types of licenses to match their edition and region. For additional information, see Edge Licensing.

3. Select **Add Another Partner** to create another new Partner, or select **Add Partner**.

   The new Partner name displays on the **Manage Partners** page. You can select the Partner name to navigate to the Partner portal and add additional configurations to the Partner. For additional information, see Configure Partner.

9.2 Configure a Partner

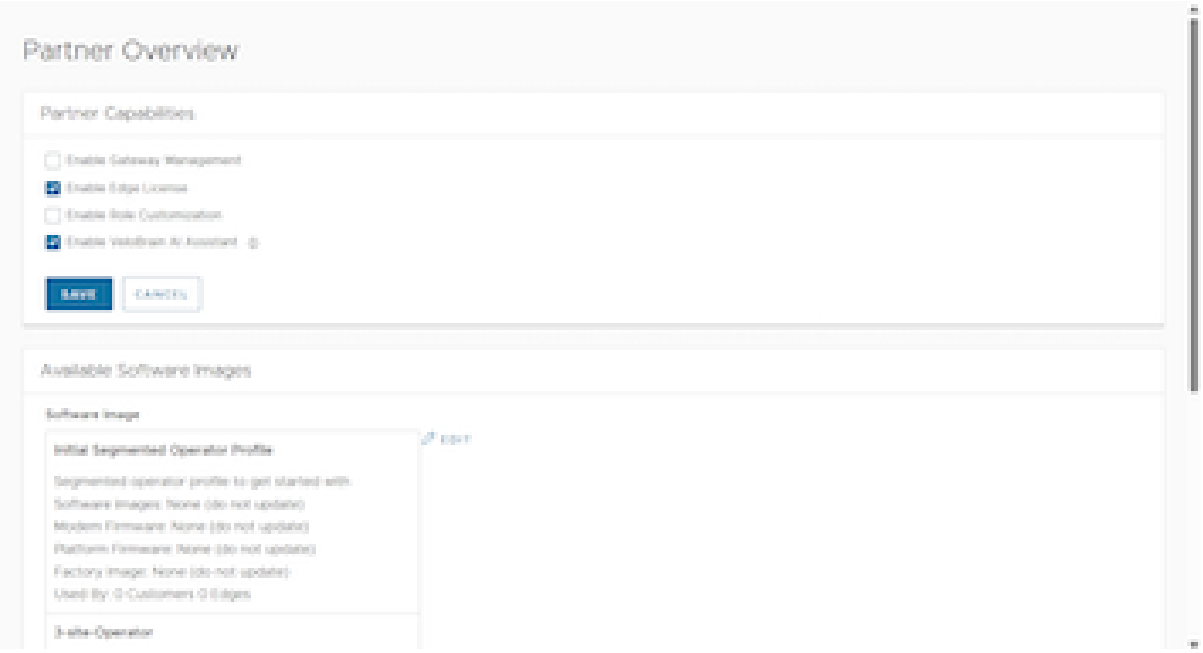
Creating a new Partner automatically triggers a redirection for Operator Superusers and Operator Admins to the **Partner Overview** page. This interface allows configuration of Partner capabilities, Software images, Gateway pools and other accessible settings.

To configure Partner information for an existing Partner:

1. In the **Operator** portal of the VeloCloud Orchestrator, select **Manage Partners**, and then select the Partner name to navigate to the **Partner** portal.
2. Select **Administration** > **Partner Configuration** to add additional configurations to the Partner.

   The **Partner Overview** page for the selected Partner appears.

   Figure 9-3: Partner Overview



3. Configure the following capabilities and settings for the selected Partner:

Table 18: Partner Overview - Options and Descriptions

Option	Description
Partner Capabilities	Selecting **Edit** allows users to select the following capabilities for the current Partner: • **Enable Gateway Management:** Allows the Partner users to create, configure, and manage their own Gateways. • **Enable Edge License:** Allows the Partner users to manage their Edge Licenses. • **Enable Role Customization:** Allows a Partner Superuser to customize the service permissions of other Partner users and Enterprise users of the Partner. • **Enable VeloBrain AI Assistant:** Allows Partners to access the VeloBrain Assistant and provides them with the privilege to manage the VeloBrain feature for their Customers. Select **Save** after editing the Partner capabilities.
Available Software Images	Displays all the software images assigned to the Partner. Select **Edit** to add or remove the software images in the list. **Note:** Users cannot remove the software images that are assigned to a Customer.
Gateway Pool	Displays the Gateway pools associated with the selected Partner. Select **Edit** to add or remove the Gateway pools in the list. **Note:** Users cannot remove the Gateway Pools that are assigned to a Customer.
Other Settings	Displays the User Agreement settings only when the **User Agreement** feature is active. By default, the **User Agreement** feature is not active. To enable this feature, navigate to **System Properties** in the Operator portal and set the `session.options value.enableUserAgreements` system property to **True**. Choose to override the default display settings of the User Agreement, by selecting the **Edit** button, and then selecting relevant option from the **User Agreement Display** menu. By default, the Customer inherits the display mode set in the system properties.

4. After configuring the required Partner details, select **Save Changes**.

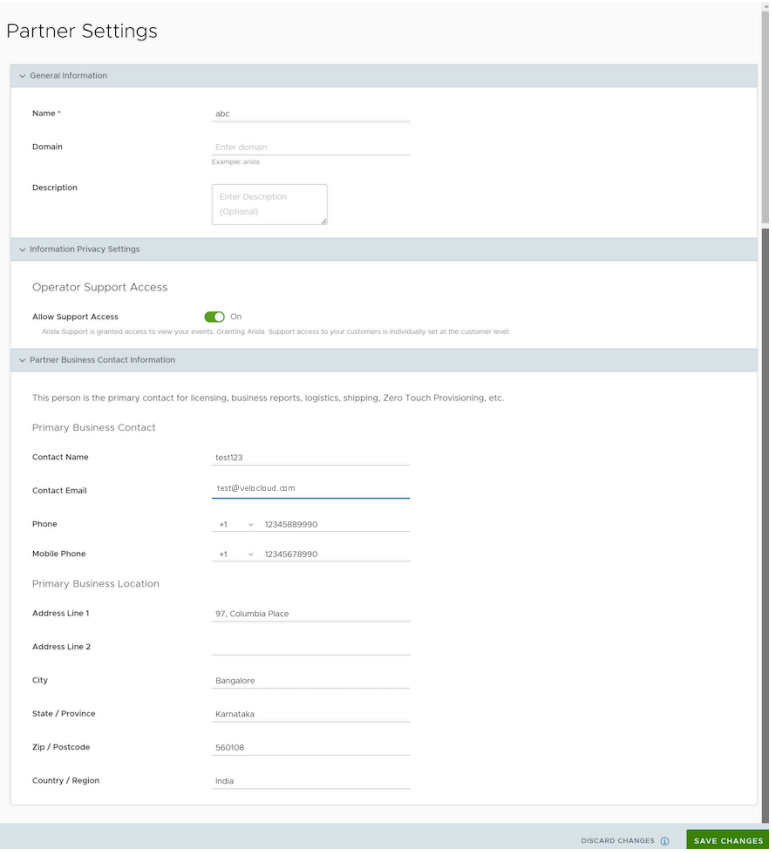
Partner Settings

As an Operator, you can configure Partner specific information such as name, primary location, and primary contact.

1. In the **Operator** portal, select **Manage Partners**. Select the link to a **Partner** name for which you want to edit the settings.
2. From the top menu, select **Administration**, and then from the left menu, select **Partner Settings**.

   The following screen appears:

   Figure 10-1: Partner Settings



3. You can edit the following settings on this screen:

Table 19: Partner Settings Option Descriptions

Option	Description
Name	You can edit the Partner name.
Domain	You can edit the Partner domain name.
Description	Enter a description. This field is optional.
Operator Support Access	This option is activated by default, indicating that Arista Support can view Partner level events.  **Note:** When deactivated, the Operator can no longer edit the settings of the selected Partner. Only the Partner can activate this setting from the Partner portal.
Partner Business Contact Information	Enter information of the primary person in charge of licensing, business reports, logistics, shipping, Edge auto-activation, etc.

4. Select **Save Changes**.

Chapter 11

Manage Operators

In the **Operator** portal, users can configure and manage Operator Profiles and Operator Users. Users can also view the events triggered by Operators.

This topic contains the following sections:

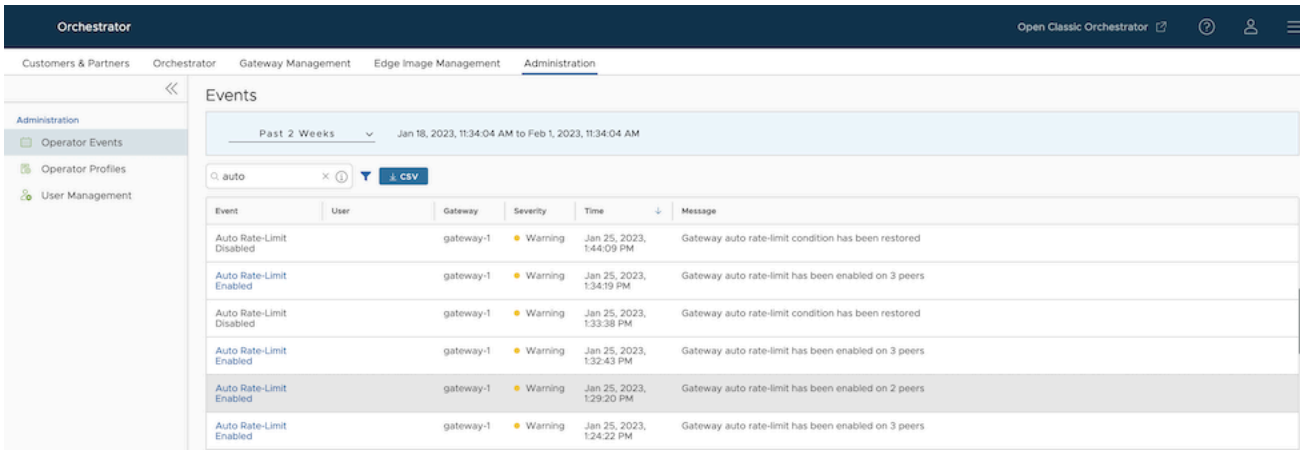
- Monitor Operator Events
- Manage Operator Profiles

11.1 Monitor Operator Events

Displays a list of events generated within the Orchestrator at the **Operator** level. These events help to determine the status of the system.

To view the Operator events using the **Orchestrator UI**, select **Administration** > **Operator Events**.

Figure 11-1: Monitor Operator Events

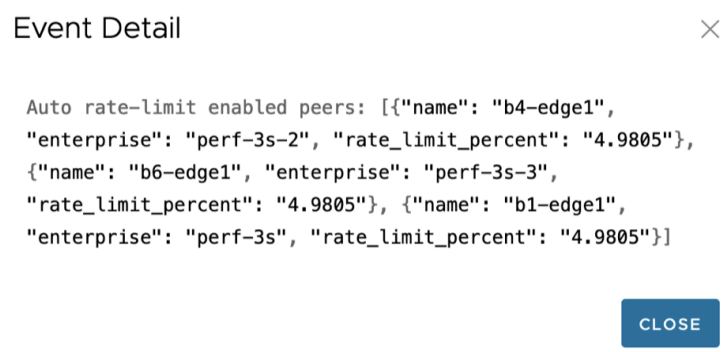


The **Events** page displays the recent Operator events. You can select the link to an event to view additional details about the selected event.

When the auto rate-limit capability is activated on a Gateway, the Gateway will drop packets if it detects that certain Edges are sending a large amount of traffic, which might be causing the Gateway to be unstable. The

event message includes the information about the list of Edges to which the Gateway is applying the auto rate limit and the rate limit percentage.

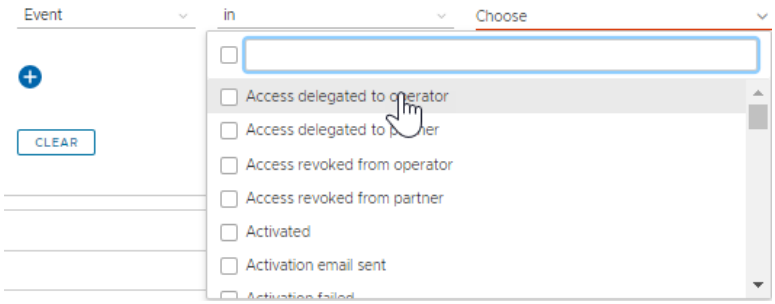
Figure 11-2: Event Detail



At the top of the page, you can choose a specific time period to view the details of events for the selected duration.

In the **Search** field, enter a term to search for specific details. Select the **Filter** icon to filter the view by a specific criteria. In the Filter, choose **Event**, and then select the drop-down arrow next to the field to view the list of **Operator Events** available and to filter by specific Events.

Figure 11-3: Filter Events



Select the **CSV** option to download a report of the events in CSV format.

Note: For detailed information about alerts and events generated within the Orchestrator at the Operator level, see Operator-Level Orchestrator Alerts and Events.

11.2 Manage Operator Profiles

An Operator Profile specifies the network settings managed by Orchestrator. After you create a Customer or Partner, you can assign an Operator profile to them.

Operators can upload, modify, or delete the following firmware and factory images in the Orchestrator UI:

- Firmware Platform images for 6x0, 7x0, and 3x00 (3400/3800/3810) Edge device models
- Firmware Modem images for 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) and 610-LTE (Edge 610LTE-AM, Edge 61LTE-RW)

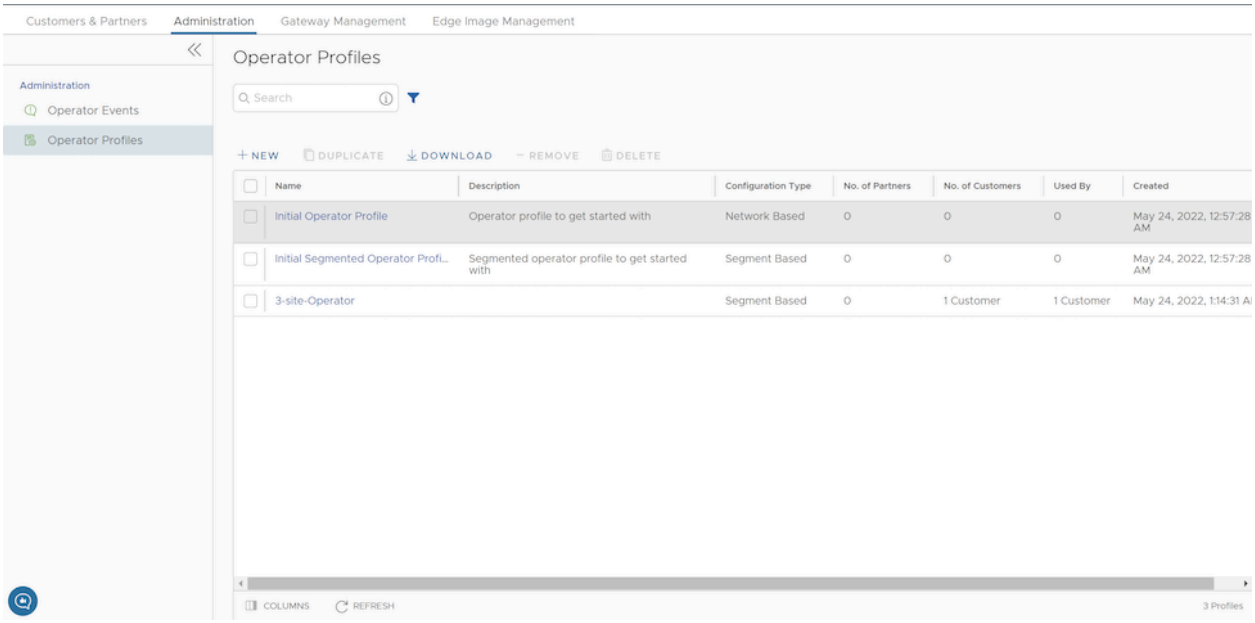
- Factory images for all physical VeloCloud Edge devices

With the 5.2 release, updating the Factory image and Platform firmware on High-availability (HA) Edges is supported. Steps and requirements are described in the appropriate sections in the procedure below.

See Platform Firmware and Factory Images for additional information.

1. In the **Operator** portal, from the top menu, select **Administration** > **Operator Profiles**.
   The **Operator Profiles** page displays the available profiles.

   Figure 11-4: Operator Profiles



   Note: The Operator profiles that contain a deprecated image are flagged to notify the user that the software version of the profile contains a deprecated software image.

2. As an Operator user, you can perform the following actions on this page:

Table 20: Operator Profiles Option Description

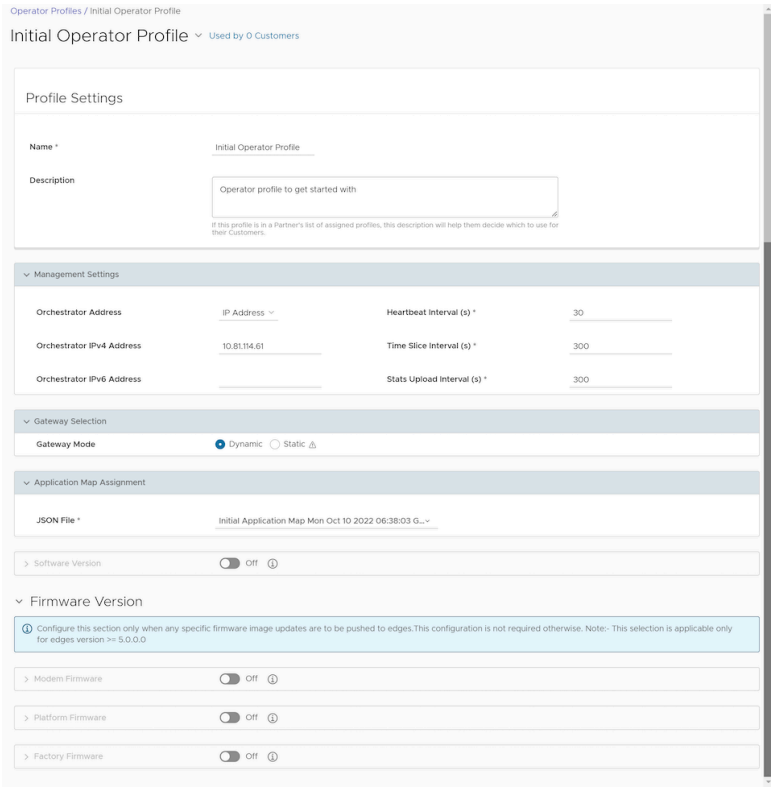
Option	Description
Search	Enter a search term to search for a matching text across the page. You can use the Advanced Search option to narrow down the search results.
New	Select this option to create a new Operator Profile. Enter the desired name and description in the dialog and select **Create**.
Duplicate	Select this option to create a copy of the selected Operator Profile. You can update the name and description.
Download	Select this option to download the csv file containing a list of all or the selected Operator Profiles.
Remove	Select this option to remove the selected Operator Profile(s) from all the associated Partners and Customers. You can complete this action only after you enter the correct number of profiles selected.
Delete	Select this option to delete the selected profile(s). You can complete this action only after you enter the correct number of profiles selected.  **Note:** You cannot delete a profile that has already been assigned to a Customer or Partner.
Columns	You can select the desired columns to be displayed in the table.
Refresh	Select this option to refresh the page.

 **Note:** You cannot delete a profile that has already been assigned to a Customer or Partner.

3. To update an existing Operator Profile, select the link to that Operator Profile name.

The selected Operator Profile page appears, as shown in the image below.

Figure 11-5: Initial Operator Profile



4. You can configure the existing settings of the selected Profile. See the following table:

Table 21: Initial Operator Profile Option Descriptions

Option	Description
Profile Settings	
Name	Edit the existing name of the Operator Profile.
Description	Edit the existing description of the Operator Profile.
Management Settings	
Orchestrator Address	Choose to use either FQDN or IP address as the Orchestrator Address. If you select FQDN, enter the FQDN address.
Orchestrator IPv4 Address	Enter the IPv4 address to be used as Orchestrator Address.
Orchestrator IPv6 Address	Enter the IPv6 address to be used as Orchestrator Address.
Heartbeat Interval (s)	Displays the time interval between the heartbeat messages sent from the Orchestrator to Edges. The default value is 30 seconds, and the minimum interval must be 10 seconds. If an Edge does not receive two consecutive heartbeats, it is marked as Down.  **Note:** When you modify the heartbeat interval, make sure to update the Edge Offline Alert Notification Delay time accordingly, to avoid sending unnecessary alerts.
Time Slice Interval (s)	Displays the time interval over which the monitoring data is collected for a flow. The default value is 300 seconds.
Stats Upload Interval (s)	Displays the time interval for uploading the monitoring data. All the data for each timeslice is collected during the Stats Upload Interval and then uploaded. The default value is 300 seconds.
Gateway Selection	
Gateway Mode	By default, the Gateway selection is Dynamic, and the VeloCloud Gateways are chosen dynamically from the Gateway Pool.Ensure that the Gateway Pool consists of at least 2 VeloCloud Gateways to ensure efficient Gateway selection. Select the checkbox to make the Gateway selection Static. For the Static Gateway selection, you must specify the Primary Gateway. You can also enter an optional Secondary Gateway.  **Note:** Use the Static Gateway Selection only for testing or debugging purposes. You must not use this option for Edge-to-Edge VPN or Partner handoff configurations.
Application Map Assignment	
JSON File	By default, the initial Application Map is assigned to the Operator Profile. You can choose a different Application Map from the drop-down list. For additional information, see Application Maps.
Software Version: You can choose to push the latest Software Image to the Edges. By default, no updates are applied to the devices. Activate the toggle button to display the following fields.	
Version	Choose the Software Image from the drop-down list. For additional information on the Software Images, see Software Images.
Update Duration	Select the **Update Duration** checkbox, and then enter the duration time in minutes. When you activate this option, the Orchestrator updates all the devices associated with the Enterprise customer within the specified time duration.
Firmware Version	
 **Note:** This section is available only for Edge versions 5.0.0 and above. To access this section, deactivate the **Software Version** section.	

The 5.1.0 release introduces the functionality for Operators to manage image upgrades for both Platform firmware, Modem firmware, and Factory Default images. (See table below for specific device requirements.

See the table below for device requirements and a description of both software types.

Table 22: Device Requirements

Software Type	Device Requirements	Components of the Edge that will be Updated
Modem Firmware	For the 5.1.0 release and later: 510-LTE (EDGE 510LTE-AE, EDGE510LTE-AP) and 610-LTE (EDGE610LTE-AM, EDGE61LTE-RW)	Carrier firmware and configuration files
Platform Firmware	For the 5.0.0 release, only Edge 6x0 devices are supported. For the 5.1.0 release, EDGE3400/ EDGE3800/ EDGE3810 models are also supported. Starting from the 5.2.4 release, Edge 7x0 devices are supported.	• BIOS (Basic Input/Output System) • CPLD (Complex Programmable Logic Device) • PIC (Programmable Intelligent Compute)
Factory Default (MR): Edge 500, Edge 5x0, Edge 6x0, Edge 7x0	For the 5.0.0 and later releases: all Edge devices.	Default factory image will be updated.

Note:

- You must update the software version first. Then, after completion, update the firmware (Platform or Modem), and then update the factory default. Do not update the software version, the firmware, and the factory default at the same time. Also, only update one component at a time.

  CAUTION: For the "Factory Image Update" feature, only use images that have been officially distributed as supported Factory Image versions. Do not use any other software update images with this feature. At any given time, Arista has an official ***current*** Factory Image version that is distributed from activate-sdwan.arista.com. Any other version (older or newer, supported or unsupported) that is installed as a ***factory image*** will be automatically updated to this version the next time the Edge is in an unactivated state and connected to the Internet.

- For releases prior to 5.0.0, the Operator Profile update will succeed, but the Firmware images will not be applied to the Orchestrator. No events will be generated, as the Orchestrator does not have a supported software version.
- For the 5.0.0 release and later, the Operator Profile update will succeed, and the Orchestrator will update the Firmware and Factory image components.

See the table below for a compatibility matrix of supported images for the supported Edge devices.

Table 23: Supported Images

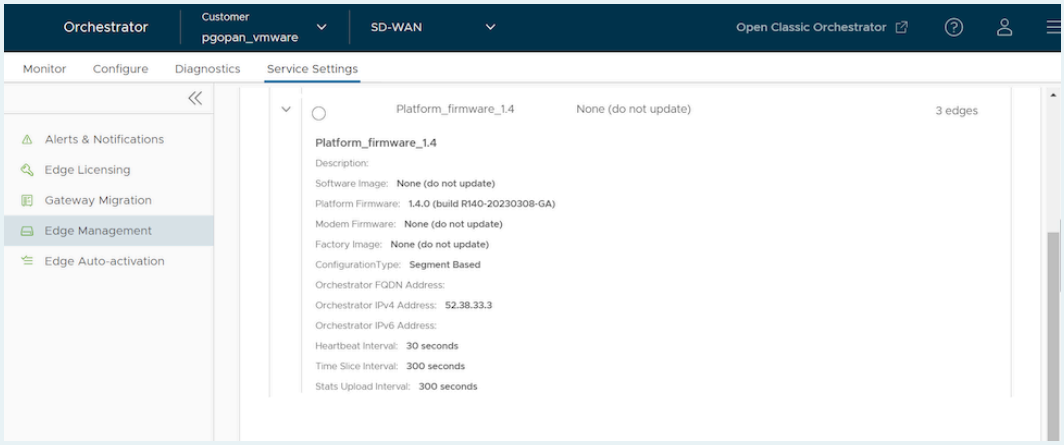
Device Family	Software Image (Device Family)	Platform Firmware (Device Family)	Modem Firmware (Device Family)	Factory Default (Device Family)
EDGE 6x0	EDGE 6X0	EDGE 6X0	610-LTE	EDGE 6X0
EDGE 3x00	EDGE 8X0 EDGE 1000 EDGE 3X00	Edge 3X00	NA	EDGE 8X0 EDGE 1000 EDGE 3X00
510LTE	Edge 510LTE-AE Edge 510LTE-AP	NA	Edge 510LTE-AE Edge 510LTE-AP	Edge 5X0
610-LTE	Edge 610LTE-AM Edge 61LTE-RW	Edge 6X0	Edge 610LTE-AM Edge 61LTE-RW	Edge 6X0
EDGE 7x0 (EDGE 710-W, EDGE 710-5G, EDGE 720, EDGE 740)	EDGE 7x0	EDGE 7x0	EDGE 7x0	EDGE 7x0

The Operator can create multiple different profiles and select profiles with various combinations to manage different types of Firmware updates to be applied to Edges. See the notes below for additional information.

Note:

- Before an Operator can update and manage the Platform Firmware for 6X0 Edge devices and Factory Default images for all devices, the Edge and Orchestrator software version must first be updated to 5.0.0 or later.
- In the 5.0.0 release, the Operator Profile name will display as an image bundle (software and firmware) listing the details of the Firmware images tagged to the Operator profile. (To view this setting, go to **Edge Management** > **Service Settings**.) See image below.

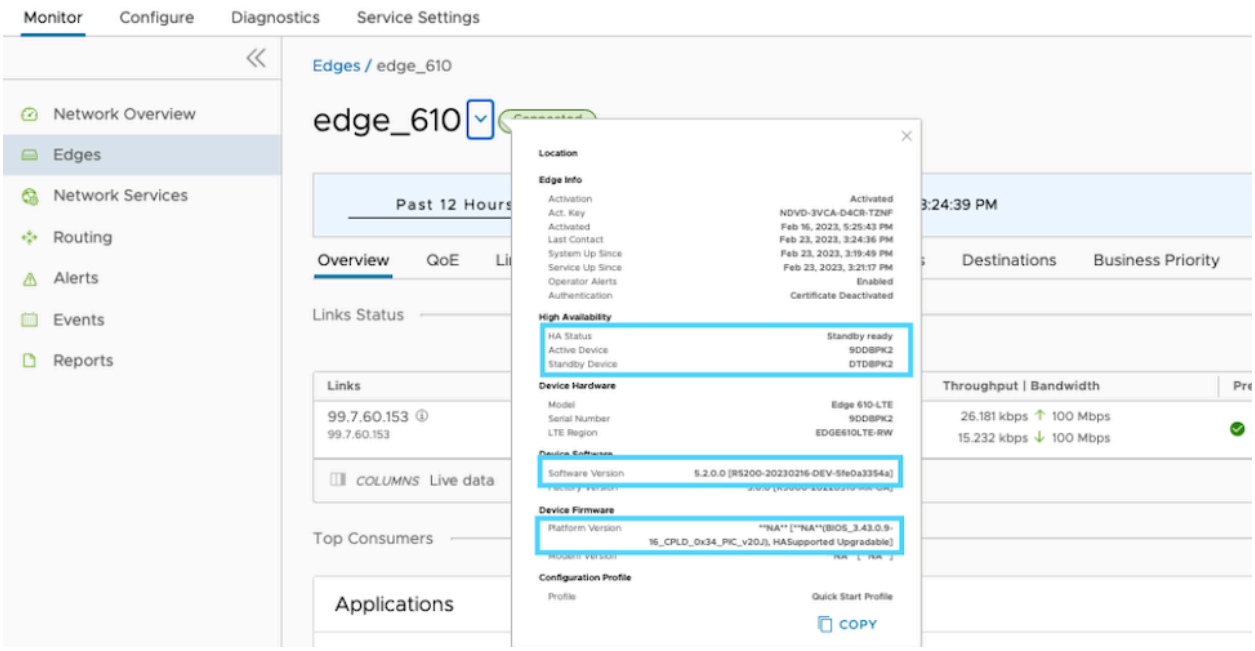
  Figure 11-6: Configure Service Settings



- All Factory and Firmware upgrades are limited to post-activation.

- The 5.0.0 software image is used to update the Factory default image on the Edge if the 5.0.0 or greater release image is uploaded from the **Software** tab. The software is updated. If the image is uploaded from the **Firmware** tab, the Factory Default image is updated. Platform Firmware images can be uploaded only from the **Firmware** tab.
- The Platform Firmware upgrade takes at least 10 minutes to complete and involves multiple Edge reboots, during which the Edge will display as offline.
- For the 5.2 release, updating the Factory image and Platform firmware on HA (High-availability) Edges is supported. For updating the Modem firmware on HA Edges, follow the steps below.
  a. The Edges must be unconfigured from HA.
  b. Apply the Modem firmware.
  c. Reconfigure to HA mode.

Figure 11-7: Monitor Edges



5. In the **Software Version** section, select the **Version** drop-down menu. Select the software image and select **Save Changes**.

   To update a Platform Firmware, a 5.0.0 or above software version for an Edge 6X0 or Edge 3X00 must be applied. To update Modem Firmware, a 5.0.0 or above software version for an Edge 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) or 610-LTE (Edge 610LTE-AM, Edge 61LTE-RW) must be applied.

Note: You must update the software version first. Then, after completion, update the Factory image or Platform, or Modem Firmware. Do not update the software version and the firmware at the same time.

Note: The Version drop-down menu displays the software images that are deprecated with a flag, but you will not be able to select the deprecated images.

For the selected profile, the usage information, such as the number of customers using the profile and the software version used by the profile, appears at the left-hand bottom of the page.

If a Software Version 5.0.0 and above for an Edge 6X0 is selected from the Software Version drop-down menu, the Firmware section is available for upgrade. If a software version lower than 5.0.0 is selected, or when a software image bundle for a Virtual Edge is selected, the Firmware section is grayed out.

6. Select **Save Changes**.
7. In the **Software Version** section, deselect the **Software Version** checkbox and select **Save Changes**.
8. In the **Firmware** section, check the Platform Firmware or Factory Image checkboxes in the appropriate sections and choose an image from the drop-down menu.

   Note: The **Firmware** image section can be configured for the software version 5.0.0 and greater, and for 6X0 Edge devices.

9. Select **Reapply** to force re-update of the selected software image for the Edges associated with the selected Operator Profile.
10. Select **Save Changes**.

Related Links

- To assign a profile for a new customer, see Create New Customer.
- To change the profile for an existing customer, see Configure Customers.
- To assign a profile for a partner, see Manage Partners.

Chapter 12

Link Insights

Release 7.0.0 introduces the **Link Insights** feature, which provides comprehensive visibility into the health and performance of WAN links across VeloCloud SD-WAN. By continuously monitoring link-level Quality of Experience (QoE) metrics, including latency, jitter, and packet loss, Link Insights identifies degraded connections and quantifies the effectiveness of SD-WAN optimization. This feature provides insights into Edges across an Enterprise, helping optimize network performance, troubleshoot, manage costs, and improve the user experience.

Key Capabilities:

- **Real-time degradation detection:** Automatically classifies link quality events as Critical (Red) or Fair (Yellow) based on configurable thresholds for Voice, Video, and Transactional traffic types.
- **Before vs. After SD-WAN comparison:** Compares link performance before and after applying SD-WAN corrective actions to quantify the overlay's mitigation impact.
- **Multi-dimensional analysis:** Groups degradation data by individual Link, Edge, or ISP to isolate problem areas across the network.
- **Top-N ranking:** Surfaces the worst-performing Links, Edges, and ISPs to focus troubleshooting on the most impactful issues.
- **Detailed drill-down:** Provides a paginated detail grid with per-link metrics, sorting, filtering, and CSV export for offline analysis and reporting.

Link Quality Classification:

Link Insights classifies link quality into three states based on QoE threshold violations:

Table 24: Link Quality Classification

State	Color	Severity	Description
Critical	Red	High	Link metrics exceed the critical threshold, causing the link to degrade severely, resulting in a noticeable impact on end users. This state requires immediate investigation.
Fair	Yellow	Moderate	Link metrics exceed the fair threshold but remain below the critical threshold, causing the link to experience moderate degradation that may affect sensitive applications.
Normal	Green	None	Link metrics are within acceptable thresholds. The Orchestrator does not detect any degradation.

Enabling Link Insights:

The **Link Insights** feature is available to Operators, Partners, and Customers. However, Operators must enable this feature for Partners and Enterprise users through system properties. For more information, see the topic *List of System Properties* in the *Arista VeloCloud Orchestrator Deployment and Monitoring Guide.*

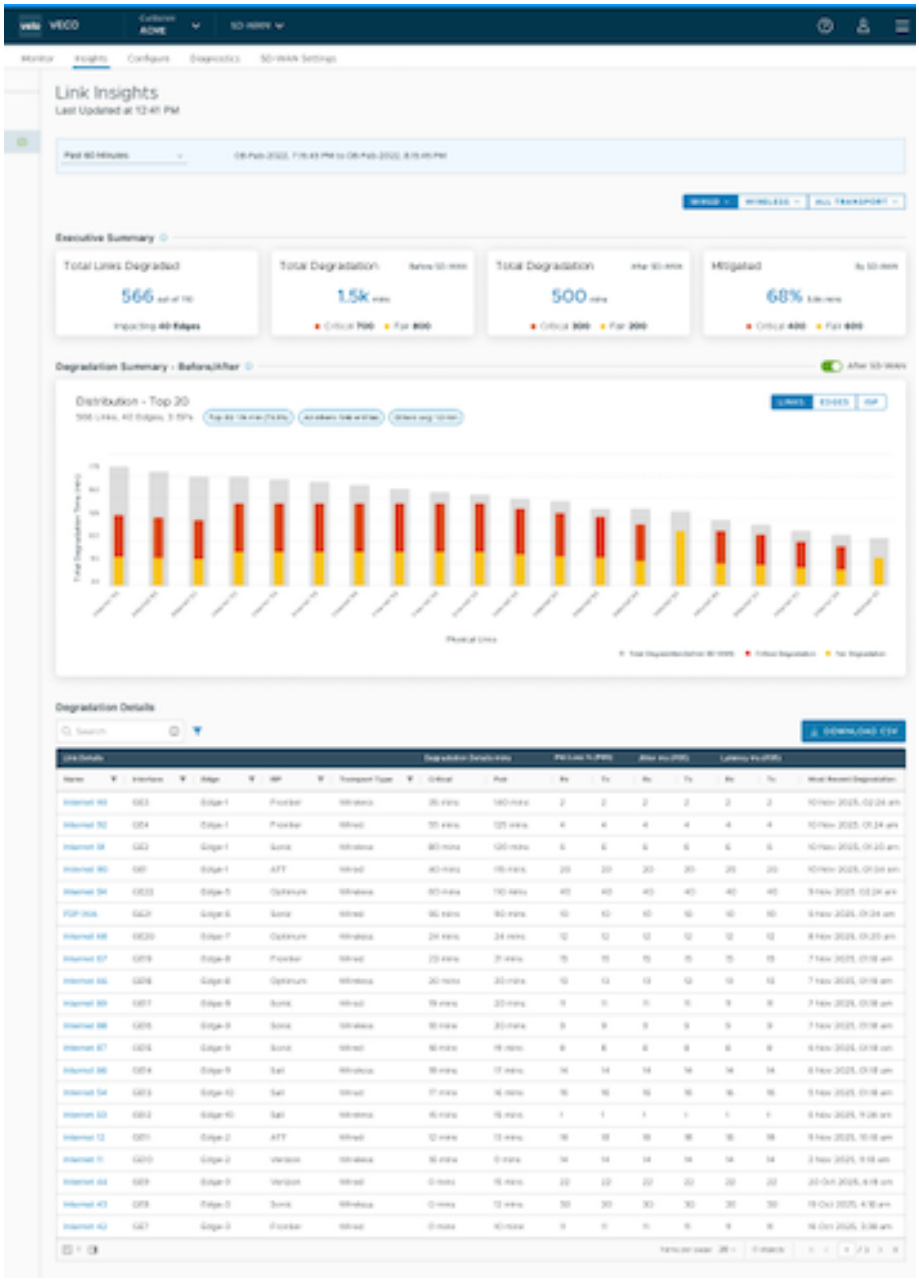
Additionally, users must activate this feature by navigating to **Global Settings** > **Customer Configuration** > **Feature Access**. For more information, see the topic *Customer Configuration* in the *Arista VeloCloud Global Settings Guide.*

Note: The **Link Insights** tab appears in Orchestrator only after completing these settings.

Accessing Link Insights

Select the **Insights** tab from the top menu of the Orchestrator. Select **Link Performance** located on the left pane. The following **Link Insights Dashboard** appears:

Figure 12-1: Link Insights Dashboard



The dashboard features three sections that offer progressively deeper levels of analysis. Click each of these links for more details.

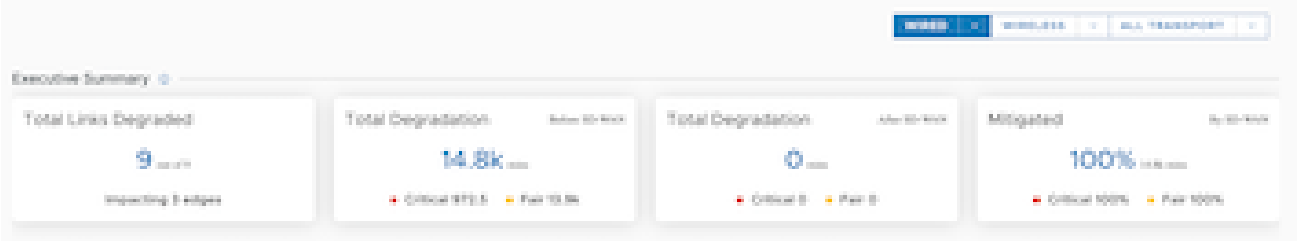
- Executive Summary
- Degradation Summary
- Degradation Details

Note: The system retains data for up to 365 days. The filter option allows users to view data based on the selected time period. Performance limitations restrict the data selection range to a maximum of 31 days. The default filter value is **Past 12 Hours**.

12.1 Executive Summary

The Executive Summary section appears at the top of the Link Insights dashboard. It displays Enterprise-wide degradation overview and SD-WAN mitigation impact.

Figure 12-2: Executive Summary



Transport Type Selection:

These buttons allow users to isolate performance data based on the physical medium of the network links:

- **Wired:** Displays metrics only for fixed-line connections. This is the default selection.
- **Wireless:** Displays metrics only for cellular or satellite connections.
- **All Transport:** Consolidates both Wired and Wireless data into a single unified view.

Note: For each transport type, users can also filter by Voice, Video, and Transactional.

The Executive Summary section displays the following data:

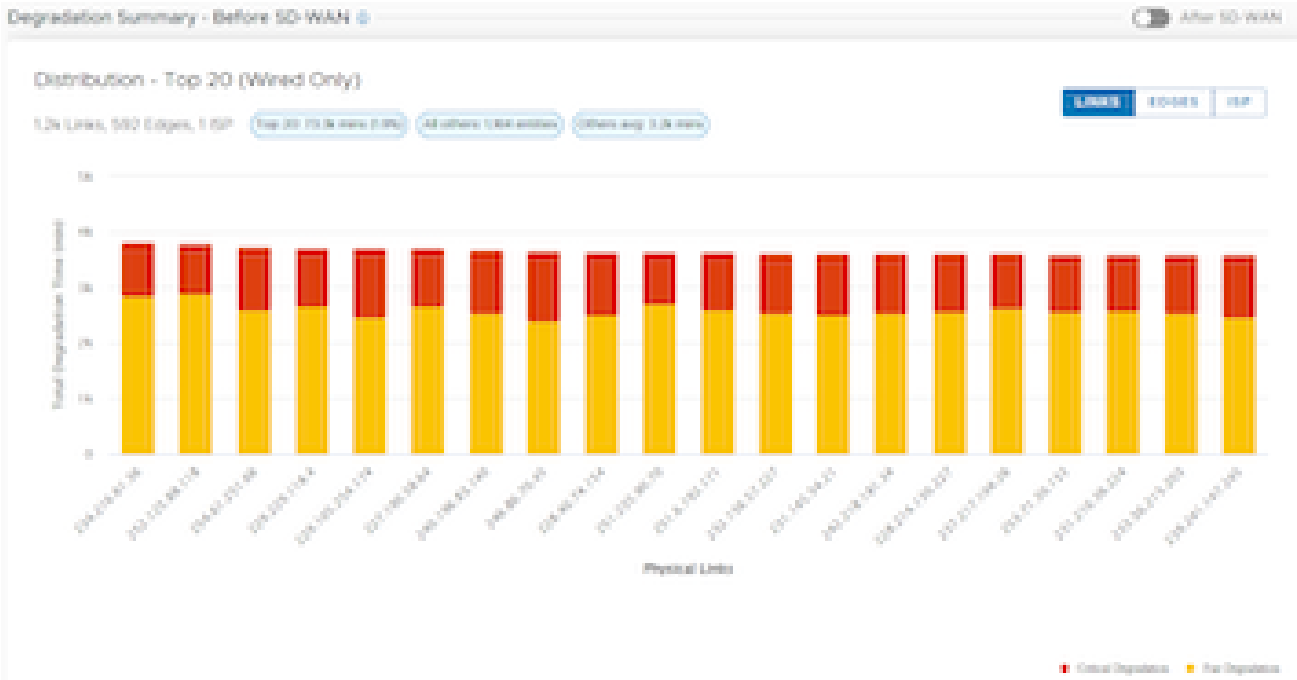
Table 25: Executive Summary - Data

Data	Description
Total Links Degraded	Number of links experiencing any degradation out of total links in the Enterprise (e.g., "200 out of 2k").
Total Degradation Before SD-WAN	Cumulative degradation time (in minutes) across all links before SD-WAN optimization.
Total Degradation After SD-WAN	Cumulative degradation time (in minutes) across all links after SD-WAN optimization.
Mitigated	Percentage of degradation time that the SD-WAN successfully eliminates. **Note:** A higher mitigation percentage indicates greater effectiveness of the SD-WAN optimization for the affected links.

12.2 Degradation Summary

The Degradation Summary section displays the cumulative degradation time, in minutes, for the selected time range. The Orchestrator measures degradation at 30-second intervals. Users can compare the link performance before and after applying the SD-WAN corrective actions. This comparison quantifies the value of the SD-WAN overlay.

Figure 12-3: Degradation Summary



Select the toggle button to switch between the **Before SD-WAN** and **After-SD-WAN** degradation summary.

- **Before SD-WAN:** Displays the raw underlay link quality measured before applying any SD-WAN corrective actions.
- **After SD-WAN:** Displays the effective link quality after applying SD-WAN corrective actions. Shows residual degradation after SD-WAN optimization. Bars that fully disappear indicate 100% mitigation.

The Degradation Summary section provides a stacked bar chart ranking the top 20 worst-performing items by total degradation time. Each bar is segmented by severity:

- Red segments represent Critical (RED) degradation time
- Yellow segments represent Fair (YELLOW) degradation time

Select one of the following tabs to filter the degradation data by Links, Edges, or ISPs:

Table 26: Degradation Filters

Tab	Description
Links	This is the default selection. Ranks individual physical links by total degradation time. Useful for identifying specific underperforming WAN connections.
Edges	Ranks Edge devices by grouping degradation across all their links. Useful for identifying sites with systemic connectivity issues.
ISPs	Ranks Internet Service Providers by grouping degradation across all links they serve. Useful for evaluating carrier performance.

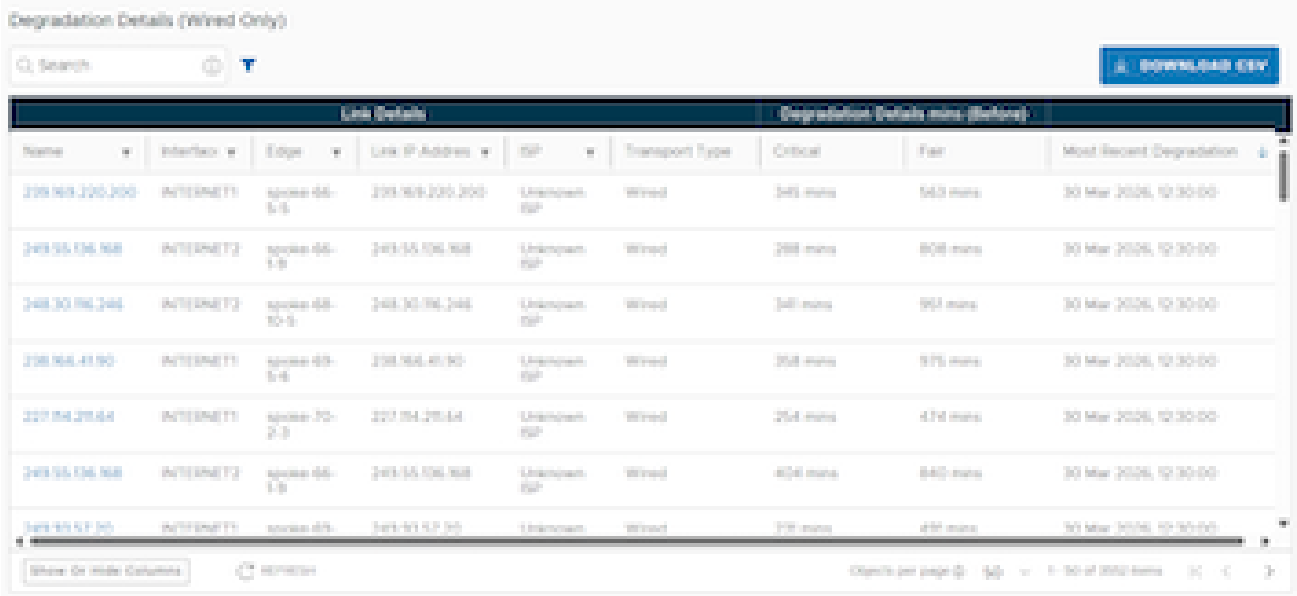
Note: At the bottom of the Degradation Summary section, three dots indicate the link statuses. The **After SD-WAN** view displays a light blue dot, which signifies that the SD-WAN overlay successfully resolved all link degradation.

Select any item from the Top 20 Links, Edges, or ISPs to view the respective degradation details in the next section.

12.3 Degradation Details

The Degradation Details section provides a paginated table with per-link performance data. It supports sorting, filtering, column selection, and CSV export for detailed analysis. Users can also refresh the data.

Figure 12-4: Degradation Details



The following columns are visible by default:

Table 27: Default Columns

Column Name	Description
Name	Name of the WAN link.
Interface	Network interface associated with the link.
Edge	Name of the Edge device.
Link IP Address	IP address assigned to the link.
ISP	Internet Service Provider for the link.
Transport Type	Type of transport (Wired or Wireless).
Critical (Before)	Total Critical (Red) degradation time before SD-WAN optimization, in minutes.
Fair (Before)	Total Fair (Yellow) degradation time before SD-WAN optimization, in minutes.
Most Recent Degradation	Timestamp of the most recent degradation event on this link.

Enable the following columns through the **Show or Hide Columns** drop-down menu:

Table 28: Additional Column Groups

Column Group	Column Names	Description
Critical Degradation (After)	Critical, Fair	Degradation time after SD-WAN optimization, in minutes.
Packet Loss - P95 (RX | TX)	Rx, Tx	95th percentile packet loss in each direction (%).
Jitter - P95 (RX | TX)	Rx, Tx	95th percentile jitter in each direction (ms).
Latency - P95 (RX | TX)	Rx, Tx	95th percentile latency in each direction (ms).

Note: Toggling a metric column group simultaneously shows or hides both the Rx and Tx columns.

Click any column header to sort the table by that column. Click again to reverse the sort direction. Sortable columns include all degradation metrics, network metrics, transport type, and last updated timestamp.

The Degradation Details section includes a Quick Search field that performs a case-insensitive substring search across all fields simultaneously. It also supports advanced column-level filtering.

Link Insights supports exporting Degradation data to CSV format for offline analysis, reporting, or integration with third-party tools. The export action takes into account all currently applied filters and sort orders.

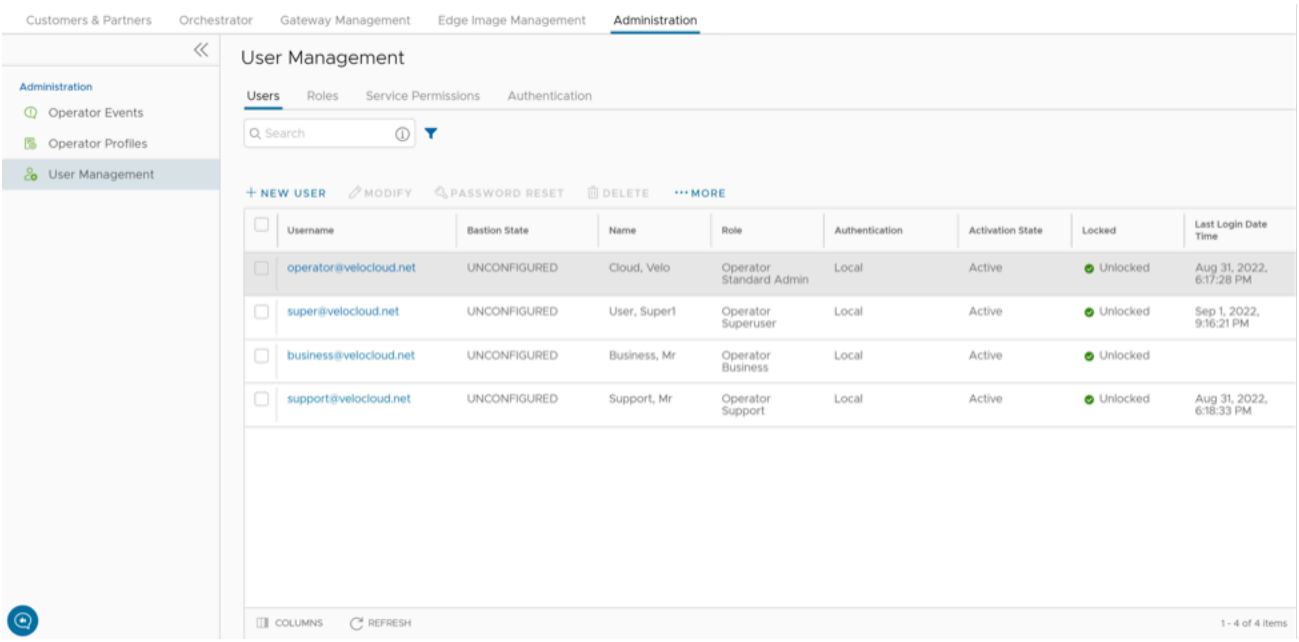
Chapter 13

User Management-Operator

The User Management feature allows you to manage users, their roles, service permissions (formerly known as Role Customization), and authentication.

As an Operator, you can access this feature from the **Operator** portal, by navigating to **Administration** > **User Management**. It displays the following screen:

Figure 13-1: User Management - Operator



The **User Management** window displays four tabs: **Users**, **Roles**, **Service Permissions**, and **Authentication**.

For additional information on each of these tabs, see:

- Users
- Roles
- Service Permissions
- Authentication

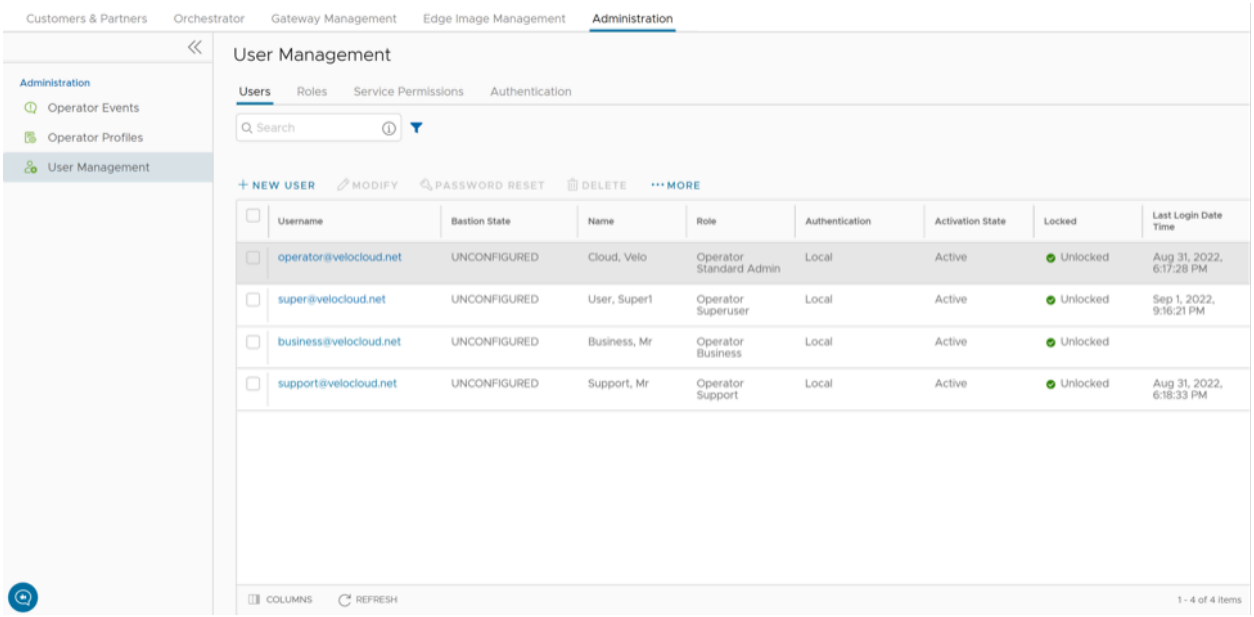
13.1 Users

As an Operator, you can view the list of existing users and their corresponding details. You can add, modify, or delete a user. However, you cannot modify or delete an Operator Superuser. An Operator Superuser can create new Operator users with different role privileges and configure API tokens for each Operator user.

To access the **Users** tab:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**. It displays the **Users** tab by default.

Figure 13-2: Users - Operator



3. On the **Users** screen, configure the following options:

Table 29: Users Option Descriptions

Option	Description
New User	Creates a new Operator user. For additional information, see Add New User.
Modify	Modifies the properties of the selected Operator user. The administrator can also select the username link to modify its properties. You can change the **Activation State** of the selected Operator user, though only an Operator Superuser can manage API tokens. For additional information, see API Tokens.
Password Reset	Sends an email to the selected user containing a link to reset their password. You can also choose to **freeze the account** until the user resets the password.
Delete	Deletes the selected user. You cannot delete the default users.
More	Select this option, and then select **Download** to download the details of all the users into a file in CSV format.

4. The following additional options are available on the **Users** tab:

Table 30: User additional Option Descriptions

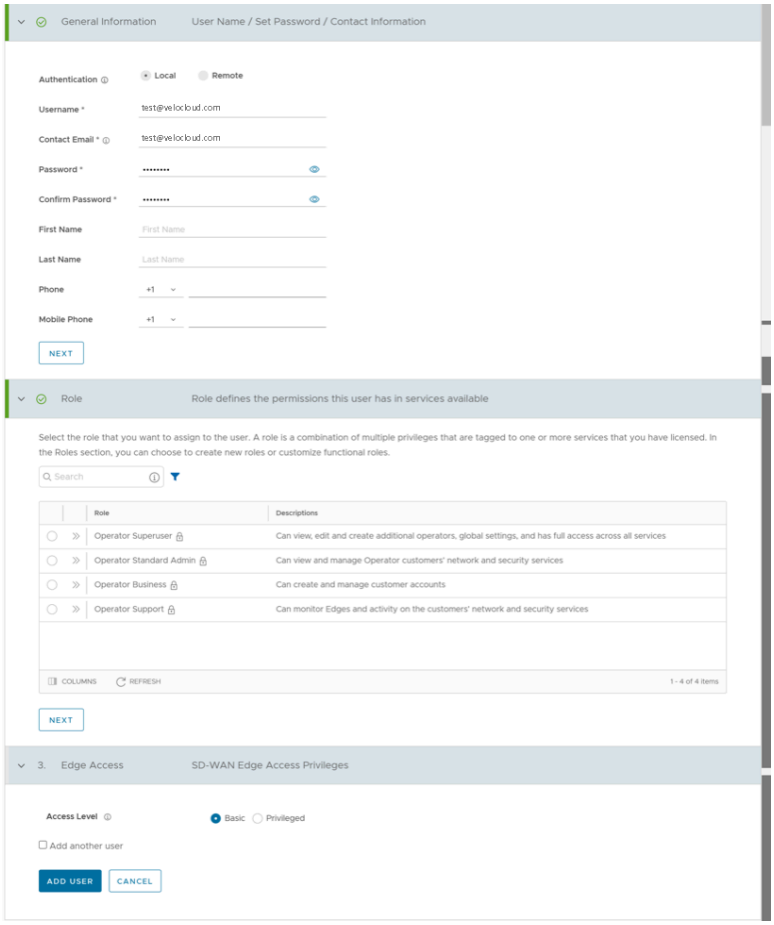
Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	you can select which columns the system displays or hides on the page.
Refresh	Select to refresh the page to display the most current data.

13.1.1 Add New User

In the **Operator** portal, you can add new users and configure the user settings. Only Operator Superusers and Operator Standard Admins can add a new user. To add a new user, perform the following steps:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**. It displays the **Users** tab by default.
3. Select **New User**. The following screen appears:

Figure 13-3: Add New User



4. Enter the following details for the new user:

Table 31: New User Option Descriptions

Option	Description
General Information	Enter the required personal details of the user.
Role	Select a role that you want to assign to the user. For information on roles, see Roles.
Edge Access	Ensure that you have Operator Superuser role to modify the Access Level for the user. Choose one of the following options: • **Basic**: Allows you to perform certain basic debug operations such as ping, tcpdump, PCAP, remote diagnostics, and so on. • **Privileged**: Grants you the root-level access to perform all basic debug operations along with Edge actions such as restart, deactivate, reboot, hard reset, and shutdown. In addition, you can access Linux shell. The default value is **Basic**. **Note:** Only Operator Superusers can modify the default value to **Privileged**.

Note: The **Next** button activates only when you enter all the mandatory details in each section.

5. Select the **Add another user** checkbox if you wish to create another user, and then select **Add User**.
   The new user appears on the **User Management** > **Users** page.
6. Select the link to the user to view or modify the details.

13.1.2 API Tokens

The administrator can access the Orchestrator APIs using tokens instead of session-based authentication. As an Operator Superuser, you can manage these API tokens and create multiple tokens for a single user.

Note: The system does not activate token-based authentication for Enterprise Read Only users or MSP Business Specialist users.

The system activates API Tokens by default. If you want to deactivate them, go to **System Properties** in the **Operator** portal, and set the value of the system property `session.options.enableApiTokenAuth` as **False**.

Note: Operator Superuser should manually delete inactive Identity Provider (IdP) users from the Orchestrator to prevent unauthorized access via API Token.

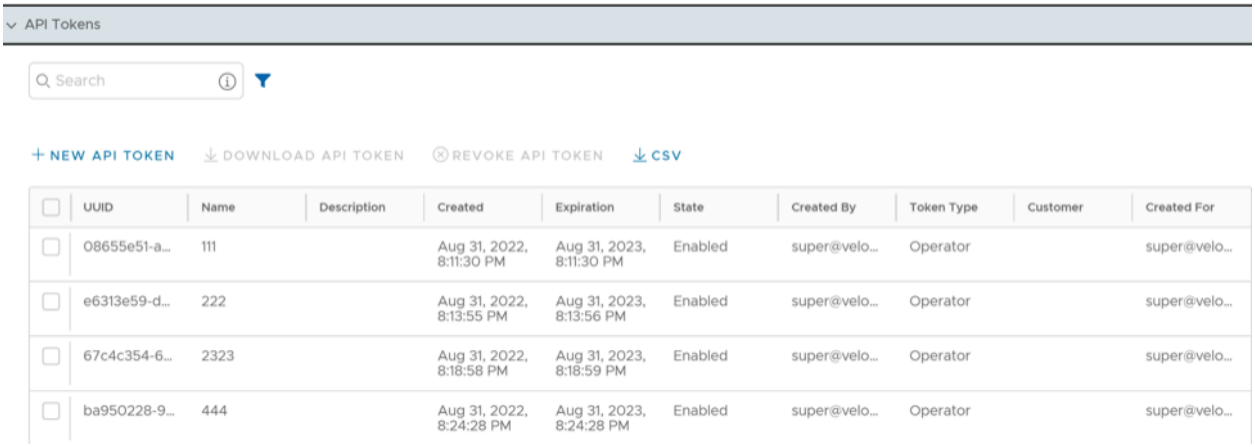
The users can create, revoke, and download the tokens based on their roles.

To manage the API tokens:

1. In the **Operator** portal, navigate to **Administration** > **User Management** > **Users**.

2. Select a user, then select **Modify** or select the link to the username. Go to the **API Tokens** section.

Figure 13-4: API Tokens



3. Select **New API Token**.

Figure 13-5: New API Token

4. In the **New Token** window, enter a **Name** and **Description** for the token, and then choose **Lifetime** from the drop-down menu.

> **Note:** When the Lifetime of the token is over, the status changes to **Expired**.

5. Select **Save**. The system displays the new token in the **API Tokens** table. Initially, the system shows the token status as `Pending`. Once you download the token, the status changes to `Enabled`.
6. To download the token, select the token, then chose **Download API Token**.
7. To deactivate a token, select the token, then choose **Revoke API Token**.

   The system shows the token status as `Revoked`.
8. Select **CSV** to download the complete list of API tokens in a `.csv` file format.

> **Note:** Only the user associated with a token can download it. After you download the token, the system displays only the Token ID. You can download a token only once. After downloading the token, the user can send it as part of the Authorization Header in a request to access the Orchestrator API.

9. You can configure the following additional options available in the **API Tokens** section:

Table 32: API Token Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Select the columns to display or hide on the page.
Refresh	Select to refresh the page to display the most current data.

The following example shows a sample snippet of the code to access an API.

```
curl -k -H "Authorization: Token <Token>"
  -X POST https://vco/portal/
  -d '{ "id": 1, "jsonrpc": "2.0", "method": "enterprise/getEnterpriseUsers", "params":
 { "enterpriseId": 1 }}'
```

Similarly, you can configure additional properties and create API tokens for Partner Admins, Enterprise Customers, and Partner Customers.

13.2 Roles

Starting from the 5.1.0 release, **Functional Roles** are renamed as **Privileges**, and **Composite Roles** are renamed as **Roles**.

The Orchestrator consists of two types of roles. The roles are categorized as follows:

- **Privileges** – Privileges are a set of roles relevant to a functionality. A privilege can be tagged to one or more services. Users require privileges to carry out business processes. For example, a Customer support role in SD-WAN is a privilege required by an SD-WAN user to carry out various support activities. Every service defines such privileges based on its supported business functionality.
- **Roles** – The privileges from various categories can be grouped to form a role. By default, the following roles are available for an Operator user:

Table 33: Roles

Role	SD-WAN Service	Global Settings Service
Operator Standard Admin	SD-WAN Operator Admin	Global Settings Operator Admin
Operator Superuser	Full Access	Full Access
Operator Business	SD-WAN Operator Business	Global Settings Operator Business
Operator Support	SD-WAN Operator Support	Global Settings Operator Support

If required, you can customize the privileges of these roles. For additional information, see Service Permissions.

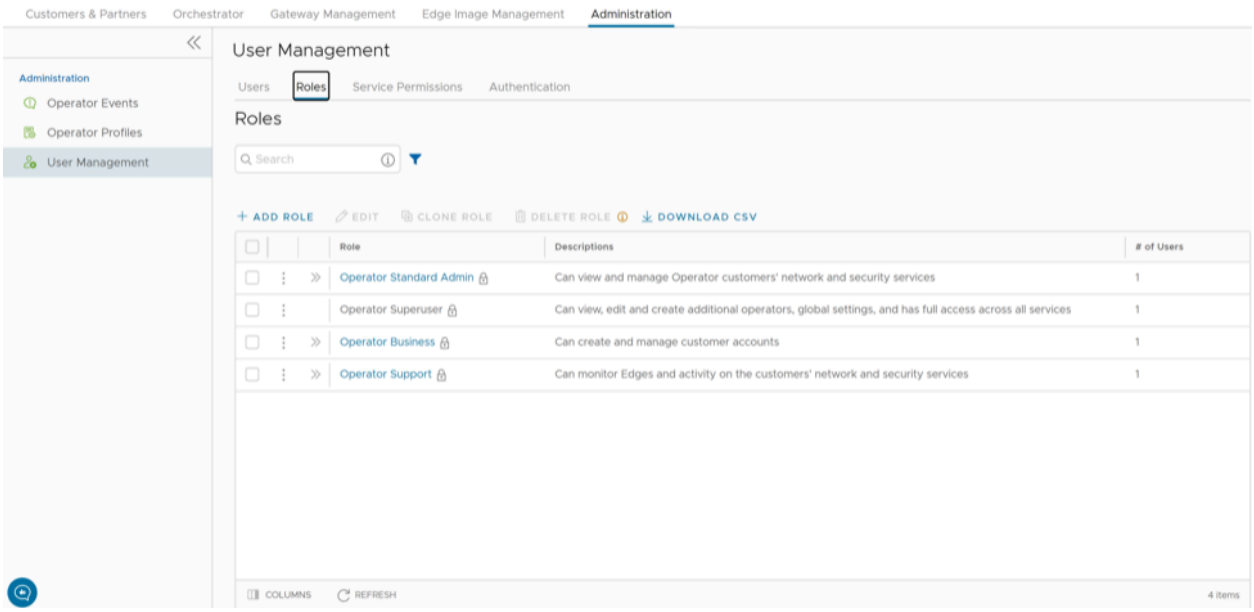
As an Operator, you can view the list of existing standard roles and their corresponding descriptions. You can add, edit, clone, or delete a new role. However, you cannot edit or delete a default role.

To access the **Roles** tab:

1. In the **Operator** portal, select **Administration** from the top menu.

2. From the left menu, select **User Management**, then choose the **Roles** tab. The following screen appears:

Figure 13-6: Roles-Operator



3. On the **Roles** screen, you can configure the following options:

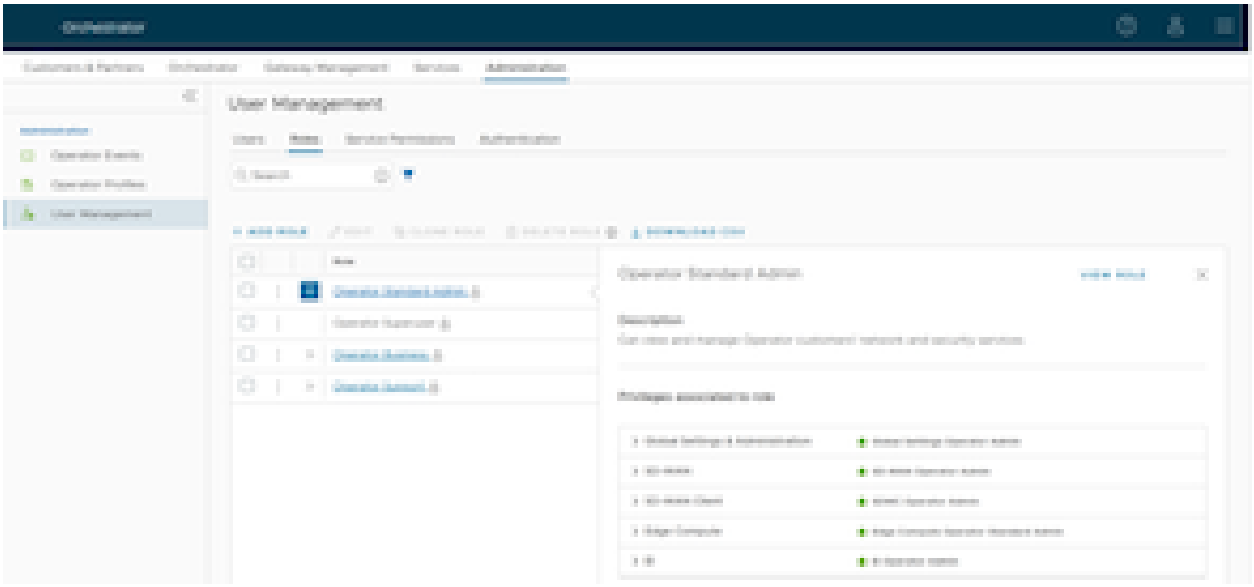
Table 34: Roles Option Descriptions

Option	Description
Add Role	Creates a new custom role. For additional information, see Add Role.
Edit	Allows you to edit only the custom roles. You cannot edit the default roles. Also, you cannot edit or view the settings of a Superuser.
Clone Role	Creates a new custom role, by cloning the existing settings from the selected role. You cannot clone the settings of a Superuser.
Delete Role	Deletes the selected role. You cannot delete the default roles. You can delete only custom composite roles. Ensure that you have removed all the users associated with the selected role, before deleting the role.
Download CSV	Downloads the details of the user roles into a file in CSV format.

Note: You can also access the **Edit**, **Clone Role**, and **Delete Role** options from the vertical ellipsis of the selected Role.

4. Select **>>** displayed before the **Role** link, to view additional details about the selected Role, as shown below:

Figure 13-7: Role Details



5. Select the **View Role** link to view the privileges associated to the selected role for the following services:
   - **Global Settings & Administration**
   - **SD-WAN**
6. The following additional options are available on the **Roles** tab:

Table 35: Additional Roles Option Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to narrow down the search results.
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

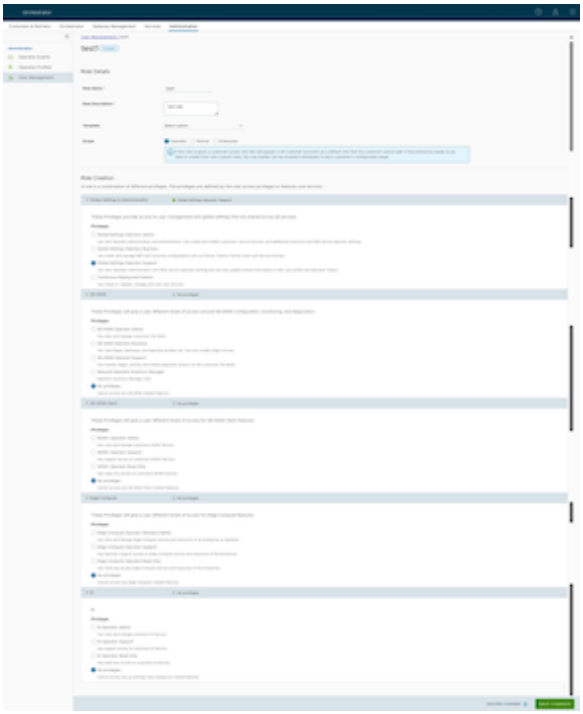
13.2.1 Add Role

To add a new role for an Operator, perform the following steps:

1. In the **Operator** portal, select **Administration**.
2. Select **User Management**, then choose the **Roles** tab.

3. Select **Add Role**. The following screen appears:

Figure 13-8: Add Role



4. Enter the following details for the new custom role:

Table 36: New Custom Role Option Descriptions

Option	Description
Role Details	
Role Name	Enter a name for the new role.
Role Description	Enter a description for the role.
Template	Optionally, select an existing role as template from the list. The privileges of the selected template become assigned to the new role.
Scope	Select **Operator**, **Partner**, or **Customer** as the scope for the new role. The new role appears in all the accounts for the selected user, as a default role. If an Operator creates a role for a Partner, it appears in the Partner's roles' list and can be edited only by an Operator and a Partner user who has the required permissions.
Role Creation: The options in this section vary depending on the selected Scope.	
Global Settings & Administration	These privileges provide access to user management and global settings that are shared across all services. Choosing one of the privileges is mandatory. By default, **Global Settings Operator Support** is selected for the **Operator** scope.
SD-WAN	These privileges provide the Operator, Partner, or Enterprise Administrator with different levels of read and/or write access around SD-WAN configuration, monitoring, and diagnostics. You can optionally choose an SD-WAN privilege. The default value is **No Privileges**.

5. Select **Save Changes**.

   The new custom role appears on the **User Management** > **Roles** page of the user, depending on the selected **Scope**.

6. Select the link to the custom role to view the settings.

13.2.2 Enterprise Security Admin Role

Starting from the 6.1.0 release, customization of the Enterprise Security Admin role is enhanced to separate network and security actions. This customization allows you to configure only the Firewall settings at Profile and Edge level. All other SD-WAN configurations become read-only for an Enterprise Security Admin role.

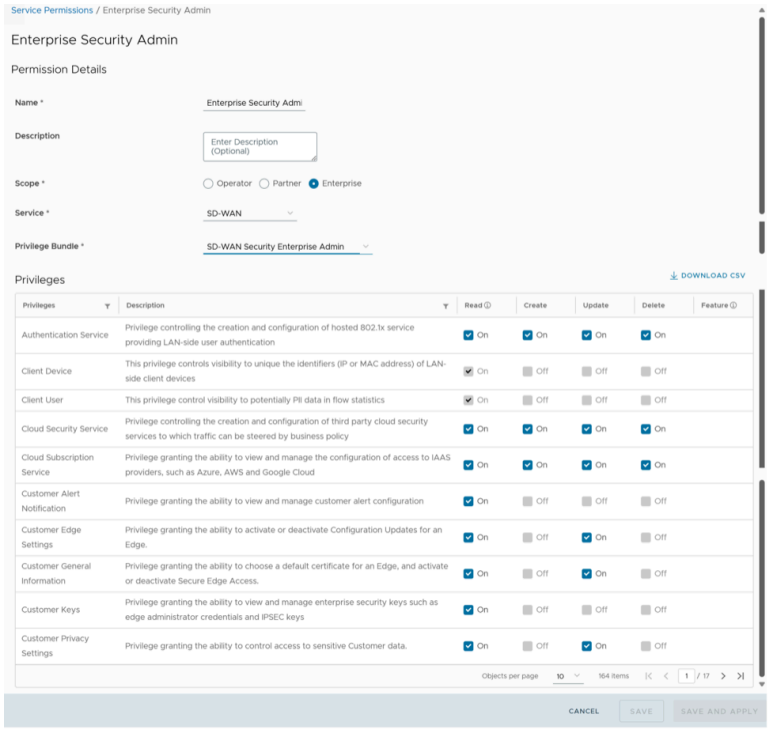
The customization of the **Enterprise Security Admin** role can be achieved by creating the following two service permissions:

- SD-WAN Enterprise Security Admin
- Global Settings Enterprise Admin

You can either create these new permissions or directly upload these permissions using JSON files. Both these methods are explained below:

1. **Create a Permission**
   a. In the **Operator** portal, select **Administration** from the top menu.
   b. From the left menu, select **User Management**, then choose the **Service Permissions** tab.
   c. Select **New Permission**. The following screen appears:

Figure 13-9: Configure Enterprise Security Admin



   d. Enter the following details to create a new permission:

Table 37: New Permission Option Descriptions

Option	Description
Name	Enter an appropriate name for the permission.
Description	Enter a description. This field is optional.
Scope	Select **Enterprise** as the scope.
Service	Select **SD-WAN** service to create the **SD-WAN Enterprise Security Admin** service permission. Select **Global Settings** service to create the **Global Settings Enterprise Admin** service permission.
Privilege Bundle	Select an appropriate privilege bundle from the drop-down menu. The privileges are populated depending on the selected Service. **Note:** Operator Superuser role is not available.
Privileges	Displays the list of privileges based on the selected **Privilege Bundle**. You can edit only those privileges that are eligible for customization.

e. Select **Download CSV** to download the list of all privileges, their description, and associated actions, into a file in CSV format.

f. Select **Save** to save the new permission. Choose **Save and Apply** to save and publish the permission. The new permission is displayed on the **Service Permissions** page.

Note: The **Save** and **Save and Apply** buttons are activated only after you modify the permissions.

2. **Upload a Permission:** You can upload a service permission by navigating to **User Management** > **Service Permissions** > **More** > **Upload Permission**.

   Below are the service permissions for **SD-WAN Enterprise Security Admin** and **Global Settings Enterprise Admin** roles with the list of privileges:

   - **SD-WAN Enterprise Security Admin**

```
{
  "roleCustomizations": [
    {
      "forRoleId": 151,
      "addPrivileges": [
        {
          "object": "EDGE_DEVICE_DEVICE_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_CLOUD_SECURITY_SERVICE",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_GLOBAL_IPV6_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_L2_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
```

```
          "object": "EDGE_DEVICE_WIFI_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_CC_FIREWALL",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_HIGH_AVAILABILITY",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_CONFIG_VISIBILITY_MODE",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_SNMP_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_SECURITY_VNF",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_NTP_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_DEVICE_ANALYTICS_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_DEVICE_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_L2_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_GLOBAL_IPV6_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_WIFI_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_CC_FIREWALL",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_CONFIG_VISIBILITY_MODE",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_NTP_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE_DEVICE_SNMP_SETTINGS",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
```

```
          "object": "EDGE_OVERVIEW",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "PROFILE",
          "action": "CREATE",
          "isDeny": 1
        },
        {
          "object": "OVERLAY_FLOW_CONTROL",
          "action": "UPDATE",
          "isDeny": 1
        },
        {
          "object": "EDGE_MANAGEMENT",
          "action": "UPDATE",
          "isDeny": 1
        }
      ],
      "removePrivileges": []
    }
  ]
}
```

- **Global Settings Enterprise Admin**

```
{
  "roleCustomizations": [
    {
      "forRoleId": 551,
      "addPrivileges": [
        {
          "object": "SYSTEM_SETTINGS_GENERAL_INFO",
          "action": "UPDATE",
          "isDeny": 1
        }
      ],
      "removePrivileges": []
    }
  ],
  "networkId": 1
}
```

For additional information, see Service Permissions.

13.3 Service Permissions

Service Permissions allow you to granularly define actions (Read, Create, Update, and Delete) assigned to each Privilege (such as Cloud Security Service and Customer Segment configuration) within a Privilege Bundle.

Note:

- Starting from the 5.1.0 release, **Role Customization** is renamed as **Service Permissions**.
- To activate this feature, an Operator user must navigate to **Global Settings** > **Customer Configuration** > **Additional Configuration** > **Feature Access**, then check the **Role Customization** checkbox.

Roles can be customized by changing the service permissions held by each role. You can customize both default roles and new roles. Roles are created based on the selected default role. Operator, Partner, and Enterprise roles are defined separately. So, there are default roles for each level, such as Operator Superuser, Partner Standard Admin, and Enterprise Support.

When customizing a role, you must select both, the user level and the role. Typically, Operator roles have more privileges by default than Partners or Enterprise Customers. When creating a user, you must assign a role to the user. Any change to that specific role's privileges is immediately applied to all users assigned to that role. Role customizations only apply to one role at a time. For example, changes to Operator Standard Admin roles do not get applied to Enterprise Standard Admin roles.

For additional information, see the topic Roles.

The Service Permissions are applied to the privileges as follows:

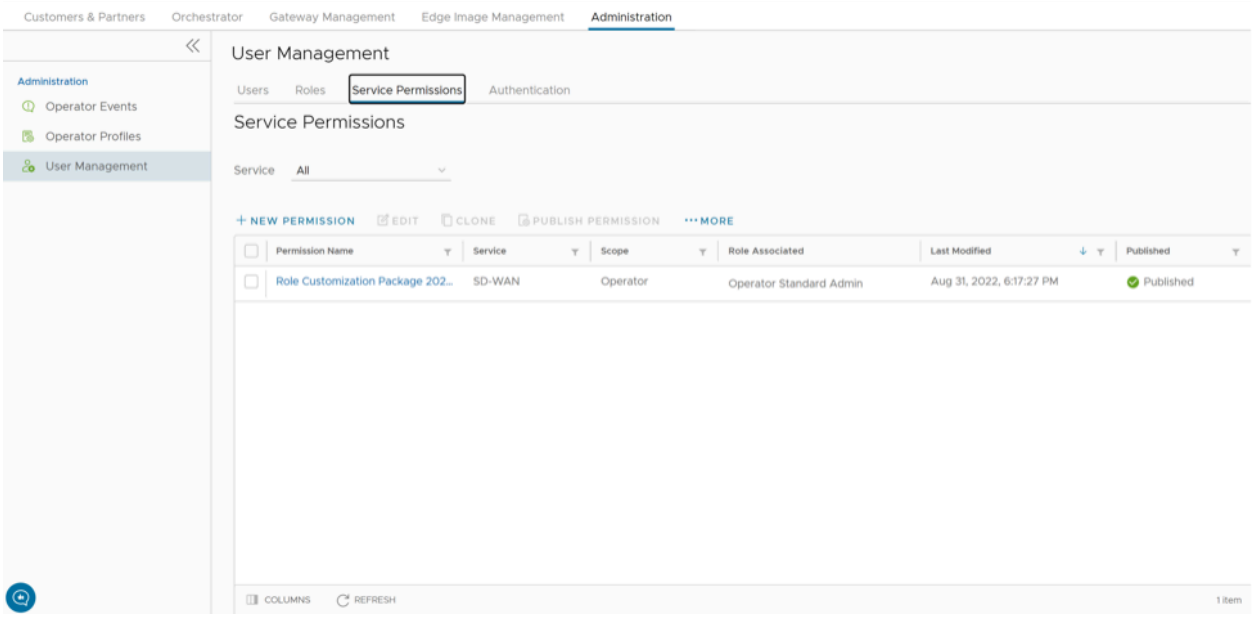
- The customizations done at the Enterprise level override the Partner or Operator level customizations.
- The customizations done at the Partner level override the Operator level customizations.
- Only when there are no customizations done at the Partner level or Enterprise level, the customizations made by the Operator are applied globally across all users in the Orchestrator.

Note: For information on user privileges, see the topic *List of User Privileges*.

To access the **Service Permissions** tab:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**, then choose the **Service Permissions** tab. The following screen appears:

   Figure 13-10: Service Permissions-Operator



3. On the **Service Permissions** screen, you can configure the following options:

Table 38: Service Permissions Option Descriptions

Option	Description
Service	Select a service from the drop-down menu. The available services are: • **All** • **Global Settings** • **SD-WAN** Each service comprises of a set of related permissions grouped together. Custom service permissions, if any, associated with the selected service are displayed. By default, all of the custom service permissions are displayed.
New Permission	Allows you to create a new set of privileges. The newly created permission is displayed in the table. For additional information, see New Permission.
Edit	Allows you to edit the settings of the selected permission. You can also select the link to the **Permission Name** to edit the settings.
Clone	Allows you to create a copy of the selected permission.
Publish Permission	Applies the customization available in the selected package to the existing permission. This option modifies the privileges only at the current level. If there are customizations available at the Operator level or a lower level for the same role, then the lower level takes precedence. For example, customizations defined by an Enterprise Superuser take precedence over customizations defined by an Operator Superuser.
More	Allows you to select from the following additional options: • **Delete**: Deletes the selected permission. You cannot delete a permission if it is already in use. **Note:** A permission can only be deleted if it is in a draft state. The **Delete** option is deactivated for a published permission. If you want to delete a published permission, you must reset the permission to system default, which changes it to draft state and activates the **Delete** option for the permission. • **Download JSON:** Downloads the list of permissions into a file in JSON format. • **Upload Permission:** Allows you to upload a JSON file of a customized permission. • **Unpublish Permissions:** Allows you to unpublish the selected permission changing it to a **Draft** state. You can modify the permission and save it again, which changes it to **Published** state.

4. The table displays the following columns:

Table 39: Option Descriptions

Option	Description
Permission Name	Displays the newly created permission.
Service	Displays the service of the new permission.
Scope	Displays the scope of the new permission.
Role Associated	Displays the associated roles using the same Privilege Bundle.
Last Modified	Displays the date and time when the permission was last modified.
Published	Displays either "Published" or "Draft" depending on the state of the permission.

5. The following additional options are available on the **Service Permissions** tab:

Table 40: Service Permissions Additional Option Descriptions

Option	Description
Columns	Select the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

Note: Service Permissions are version dependent, and a service permission created on an Orchestrator using an earlier software release will not be compatible with an Orchestrator using a later release. For example, a service permission created on an Orchestrator that is running Release 3.4.x does not work properly if the Orchestrator is upgraded to a 4.x Release. Also, a service permission created on an Orchestrator running Release 3.4.x does not work properly when the Orchestrator is upgraded to 4.x.x Release. In such cases, the user must review and recreate the service permission for the newer release to ensure proper enforcement of all roles.

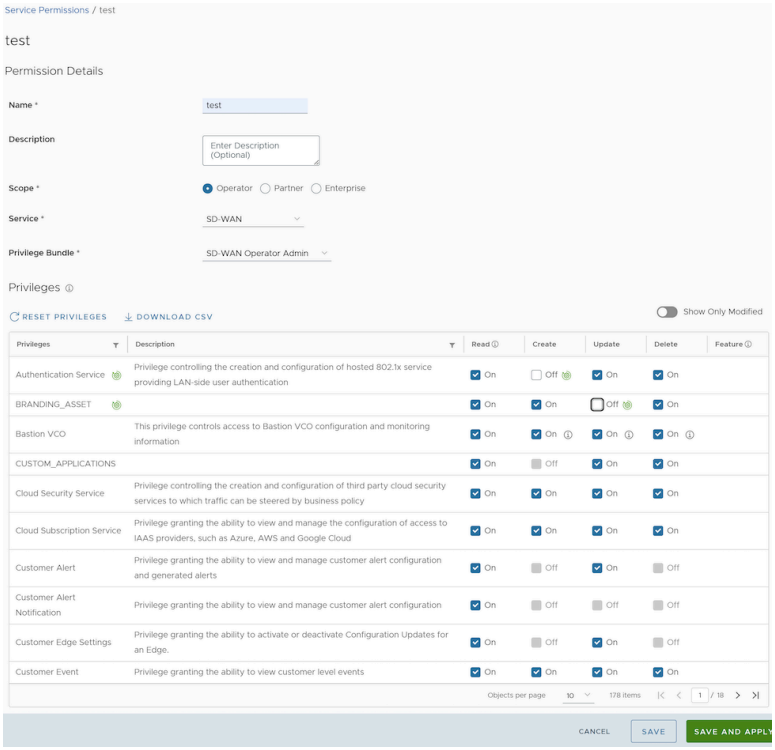
13.3.1 New Permission

You can customize the privileges and apply them to the existing permission in the Orchestrator.

To add a new permission, perform the following steps:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**, then choose the **Service Permissions** tab.
3. Select **New Permission**. The following screen appears:

Figure 13-11: New Permission



4. Enter the following details to create a new permission:

Table 41: New Permission Option Descriptions

Option	Description
Name	Enter an appropriate name for the permission.
Description	Enter a description. This field is optional.
Scope	Select **Operator**, **Partner**, or **Enterprise** as the scope. An Operator can apply the permissions for Operators, Partners, and Customers.
Service	Select a service from the drop-down menu. The available services are: • **Global Settings** • **SD-WAN**
Privilege Bundle	Select a privilege bundle from the drop-down menu. The privileges are populated depending on the chosen **Service**.
Privileges	Displays the list of privileges, in a tabular format, based on the selected **Privilege Bundle**.

To activate or deactivate a specific privilege, select or deselect the corresponding checkbox in the **Privileges** table. The available checkboxes are **Read**, **Create**, **Update**, and **Delete**.

Starting from the release 6.4.0, a green icon is displayed whenever a privilege is modified. This icon is displayed next to the modified checkbox and the privilege name.

Some privileges do not support selection of an independent action. In this case, if you select any one action checkbox, all the other checkboxes get selected too. A tool tip is provided for such privileges. Also, the **Read** action checkbox does not allow independent selection. When selected, all the other checkboxes for that particular privilege also get automatically selected.

Note: You can edit only those privileges that are eligible for customization. Operator Superuser role cannot be customized.

5. Slide the **Show Only Modified** toggle button, located at the top right of the privileges table, to view only the modified privileges.
6. Select **Reset Privileges** to reset all the changes.
7. Select **Download CSV** to download the list of all privileges, their description, and associated actions, into a file in a CSV format. You can choose from the below options:

Table 42: Privileges

Default Privileges	Downloads the original privileges ignoring all the current modifications.
Modified Privileges	Downloads only the privileges that were modified.
Current Privileges	Downloads all the current privileges.

Note: If you select **Reset Privileges**, then choose **Download CSV**, the **Default Privileges** and **Current Privileges** options, both display the same list.

8. Select **Save** to save the new permission. Select **Save and Apply** to save and publish the permission.

Note: The **Save** and **Save and Apply** buttons are activated only after you modify the permissions.

The new permission is displayed on the Service Permissions page. If you create another permission using the same scope and service, the privilege displays the last modified settings by default.

13.3.2 List of User Privileges

This section lists all the privileges available in the **Operator** portal.

The columns in the table indicate the following:

- **Allow Privilege** – Do the privileges have allow access?
- **Deny Privilege** – Do the privileges have deny access?
- **Customizable** – Is the privilege available for customization in the **Service Permissions** tab?

Table 43: Available Privileges

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Manage Customers	Create Customer	Grants ability to view and manage Enterprise Customers as an Operator or a Partner	Yes	No	No
	Read Customer				
	Update Customer			Yes	Yes
	Delete Customer			No	No
	Manage Customer				
Manage Partners	Create Partner	Grants ability to view and manage Partners	Yes	No	No
	Read Partner				
	Update Partner				
	Delete Partner				
	Manage Partner				
Software Images	Create Software Package	Grants access to upload and assign Edge Software Images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
System Properties	Create System Property	Grants access to view and manage System Properties	Yes	Yes	No
	Read System Property				Yes
	Update System Property				No
	Delete System Property				No
	Manage System Property				Yes
	Edit Restricted System Properties	Controls the ability of the user to edit restricted system properties	Yes	No	No
Operator Events	Create Operator Event	Grants ability to view Operator events	Yes	Yes	Yes
	Read Operator Event				
	Update Operator Event				
	Delete Operator Event				
	Manage Operator Event				
Operator Profiles	Create Operator Profile	Grants ability to view and manage Operator profiles	Yes	Yes	Yes
	Read Operator Profile				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Update Operator Profile				
	Delete Operator Profile				
	Manage Operator Profile				
	View Tab Operator Profile	Controls ability of the user to view and configure within the Operator profile menu	No	Yes	Yes
Operator Users	Create Operator User	Grants ability to view and manage Operator administrative users	Yes	Yes	No
	Read Operator User				Yes
	Update Operator User				No
	Delete Operator User				No
	Manage Operator User				Yes
Operator Users > **API Tokens**	Create Operator Token	Grants ability to view and manage the operator Authentication Tokens	Yes	No	No
	Read Operator Token				
	Update Operator Token				
	Delete Operator Token				
	Manage Operator Token				
Gateway Pools Gateways Gateway Diagnostic bundles	Create Gateway	Grants ability to view and manage Gateway pools and Gateways as an Operator or a Partner	Yes	Yes	Yes
	Read Gateway				
	Update Gateway				
	Delete Gateway				
	Manage Gateway				
	View Tab Gateway List	Controls the ability of the user to view the list of Gateways	No	Yes	Yes
Gateways > **New Gateway**	Create Operator PKI	Grants ability to view and manage Operator level PKI configuration including Gateway certificates and certificate authority	Yes	Yes	No
Gateway > **Gateway Authentication Mode**	Read Operator PKI				Yes
	Update Operator PKI				No
	Manage Operator PKI				Yes
Gateway Diagnostic Bundles > **Download Diagnostic Bundles**	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics	No	Yes	Yes

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
Application Maps	Create Software Package	Grants access to upload and assign Edge software images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
Service Permissions	Create Service Permissions Package	Grants access to manage Service Permissions packages	Yes	No	No
	Read Service Permissions Package				
	Update Service Permissions Package				
	Delete Service Permissions Package				
	Manage Service Permissions Package				
Edge Licensing	Create License	Grants ability to view and manage Edge licensing	Yes	No	No
	Read License			Yes	Yes
	Update License				
	Delete License			No	No
	Manage License				
CA Summary > **Gateway Certificates** > **Revoke Certificate**	Read Operator PKI	Grants ability to view and manage operator level PKI configuration including Gateway certificates and certificate authority	Yes	Yes	Yes
	Delete Operator PKI				No
	Manage Operator PKI				Yes
	Read Customer PKI	Grants ability to view and manage Enterprise PKI settings	Yes	No	No
	Delete Customer PKI				
	Manage Customer PKI				
Orchestrator Authentication > **Operator Authentication**	Create Operator Authentication	Grants ability to view and manage Operator authentication mode, like SSO, RADIUS, or Native	Yes	Yes	Yes
	Read Operator Authentication				
	Update Operator Authentication				
	Delete Operator Authentication				

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
	Manage Operator Authentication				
Orchestrator Authentication > **Enterprise Authentication**	Create Customer Authentication	Grants ability to view and manage Customer authentication mode, like RADIUS or Native	Yes	Yes	Yes
	Read Customer Authentication				
	Update Customer Authentication				
	Delete Customer Authentication				
	Manage Customer Authentication				
Replication	Create Replication	Grants access to view and configure Orchestrator disaster recovery	Yes	Yes	No
	Read Replication				Yes
	Update Replication				No
	Delete Replication				
	Manage Replication				Yes
Orchestrator Diagnostics > **Diagnostic Bundles**	Create Orchestrator Diagnostics	Grants access to request and view Orchestrator diagnostic bundles	Yes	Yes	Yes
Orchestrator Diagnostics > **Database Statistics**	Read Orchestrator Diagnostics				
	Update Orchestrator Diagnostics				
	Delete Orchestrator Diagnostics				
	Manage Orchestrator Diagnostics				
Orchestrator Upgrade for Standalone	Create Software Package	Grants access to upload and assign Edge software images and Application Maps	Yes	Yes	Yes
	Read Software Package				
	Update Software Package				
	Delete Software Package				
	Manage Software Package				
Orchestrator Upgrade for DR Setup	Create Replication	Grants access to view and configure Orchestrator disaster recovery	Yes	Yes	No
	Read Replication				Yes
	Update Replication				No
	Delete Replication				
	Manage Replication				Yes

Feature	Name of the Privilege	Description	Allow Privilege	Deny Privilege	Customizable
User Agreements	Create User Agreement Read User Agreement Update User Agreement Delete User Agreement Manage User Agreement	Grants access to configure the customer user agreement	Yes	No	No
Orchestrator Owners Manage Orchestrators Edge Inventory	Create Edge Inventory Read Edge Inventory Update Edge Inventory Delete Edge Inventory Manage Edge Inventory	Grants ability to view and manage Edge inventory as needed for Redirect configuration	Yes	No	No

When the corresponding user privilege is denied, the Orchestrator window displays the `404 resource not found` error.

The following table provides a list of customizable feature privileges:

Table 44: Customizable Permissions

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Configure > **Edges** > **Select Edge**	Overview	Assign Edge Profile	Grants ability to assign a Profile to Edges
Configure > **Edges** > > **Select Edge**	Firewall	Configure Edge Firewall Logging	Grants ability to configure Edge level firewall logging
Configure > **Profiles** > **Select Profile**	Firewall	Configure Profile Firewall Logging	Grants ability to configure Profile level firewall logging
Diagnostics > **Remote Actions**	**Select Edge** > **Deactivate**	Deactivate Edge	Grants ability to reset the device configuration to its factory default state
Global Settings > **Enterprise Settings** > **Information Privacy Settings** > **SD-WAN PCI**	Enforce PCI Compliance	Deny PCI Operations	Denies access to sensitive Customer data including PCAPs, etc. on the Edges and Gateways, for all users including Arista Support
Diagnostics > **Diagnostic Bundles**	**Select Edge** > **Download Bundle**	Download Edge Diagnostics	Grants ability to download Edge Diagnostics
Gateway Management > **Diagnostic Bundles**	**Select Gateway** > **Download Bundle**	Download Gateway Diagnostics	Grants ability to download Gateway Diagnostics
Configure > **Profiles**	Duplicate	Duplicate Customer Profile	Grants ability to edit duplicate customer level Profiles
Configure > **Segments / Configure** > **Profiles / Configure** > **Edges**	Segments drop-down menu	Edit Tab Segments	Grants ability to edit within the Segments tab
Configure > **Edges** > **Select Edge**	Device	Enable HA Cluster	Grants ability to configure HA Clustering
Configure > **Edges** > **Select Edge**	Device	Enable HA Active/Standby Pair	Grants ability to configure active/standby HA
Configure > **Edges** > **Select Edge**	Device	Enable HA VRRP Pair	Grants ability to configure VRRP HA
Diagnostics > **Remote Diagnostics**	Clear ARP Cache	Remote Clear ARP Cache	Grants ability to clear the ARP cache for a given interface
Diagnostics > **Remote Diagnostics** > **Gateway**	Cloud Traffic Routing (drop-down menu)	Remote Cloud Traffic Routing	Grants ability to route cloud traffic remotely
Diagnostics > **Remote Diagnostics**	DNS/DHCP Service Restart	Remote DNS/DHCP Restart	Grants ability to restart the DNS/DHCP service
Diagnostics > **Remote Diagnostics**	Flush Flows	Remote Flush Flows	Grants ability to flush the Flow table, causing user traffic to be re-classified
Diagnostics > **Remote Diagnostics**	Flush NAT	Remote Flush NAT	Grants ability to flush the NAT table
Diagnostics > **Remote Diagnostics** > **LTE SIM Switchover**	LTE Switch SIM Slot **Note:** This is for 610-LTE and 710 5G devices only.	Remote LTE Switch SIM Slot	Grants ability to activate the SIM Switchover feature. After the test is successful, you can check the status from Monitor > Edges > Overview tab
Diagnostics > **Remote Diagnostics**	List Paths	Remote List Paths	Grants ability to view the list of active paths between local WAN links and each peer
Diagnostics > **Remote Diagnostics**	List current IKE Child SAs	Remote List current IKE Child SAs	Grants ability to use filters to view the exact Child SAs you want to see

Navigation Path in the Enterprise Portal	Name of the Tab	Name of the Privilege	Description
Diagnostics > **Remote Diagnostics**	List current IKE SAs	Remote List Current IKE SAs	Grants ability to use filters to view the exact SAs you want to see
Diagnostics > **Remote Diagnostics**	MIBs for Edge	Remote MIBS for Edge	Grants ability to dump Edge MIBs
Diagnostics > **Remote Diagnostics**	NAT Table Dump	Remote NAT Table Dump	Grants ability to view the contents of the NAT table
Diagnostics > **Remote Diagnostics**	**Select Edge** > **Rebalance Hub Cluster**	Remote Rebalance Hub Cluster	Grants ability to either redistribute Spokes in Hub Cluster or redistribute Spokes excluding this Hub
Diagnostics > **Remote Diagnostics**	**Select Edge (with SFP module)** > **Reset SFP Firmware Configuration**	Remote Reset SFP Firmware Configuration	Grants ability to reset the SFP Firmware Configuration
Diagnostics > **Remote Actions**	Reset USB Modem	Remote Reset USB Modem	Grants ability to execute the Edge USB modem reset remote action
Diagnostics > **Remote Diagnostics**	Scan for Wi-Fi Access Points	Remote Scan for Wi-Fi Access Points	Grants ability to scan the Wi-Fi functionality for the VeloCloud Edge
Diagnostics > **Remote Diagnostics**	System Information	Remote System Information	Grants ability to view system information such as system load, recent WAN stability statistics, monitoring services
Diagnostics > **Remote Diagnostics**	VPN Test	Remote VPN Test	Grants ability to execute the Edge VPN test remote action
Diagnostics > **Remote Diagnostics**	WAN Link Bandwidth Test	Remote WAN link Bandwidth Test	Grants ability to re-test the bandwidth of a WAN link
Diagnostics > **Remote Actions**	**Select Edge** > **Shutdown**	Shutdown Edge	Grants ability to execute the Edge shutdown remote action
Service Settings > **Alerts & Notifications**	**Notifications** > **Email/SMS**	Update Customer SMS Alert	Grants ability to configure SMS alerts at the customer level
Monitor > **Edges** > **Select Edge**	Top Sources	View Edge Sources	Grants ability to view the Monitor Edge Sources tab
Monitor > **Firewall**	Firewall Logging	View Firewall Logs	Grants ability to view collected firewall logs
Monitor > **Edges** > **Select Edge**	Top Sources	View Flow Stats	Grants ability to view collected flow statistics
Monitor > **Firewall Logs**	Firewall Logs	View Profile Firewall Logging	Grants ability to view the details of firewall logs originating from VeloCloud Edges
Configure > **Profiles**	Firewall	View Stateful Firewall	Grants ability to view collected flow statistics
Configure > **Profiles**	**Firewall tab** > **Configure Firewall** > **Syslog Forwarding**	View Syslog Forwarding	Grants ability to view logs that are forwarded to a configured syslog collector
Operator portal > **Gateway Management**	Gateways	View Tab Gateway List	Grants ability to view the Gateway list tab
Operator portal > **Administration**	Operator Profiles	View Tab Operator Profile	Grants ability to view and configure settings within the Operator Profile menu tab
Monitor > **Edges** > **Select Edge**	Top Sources	View User Identifiable Flow Stats	Grants ability to view potential user identifiable flow source attributes

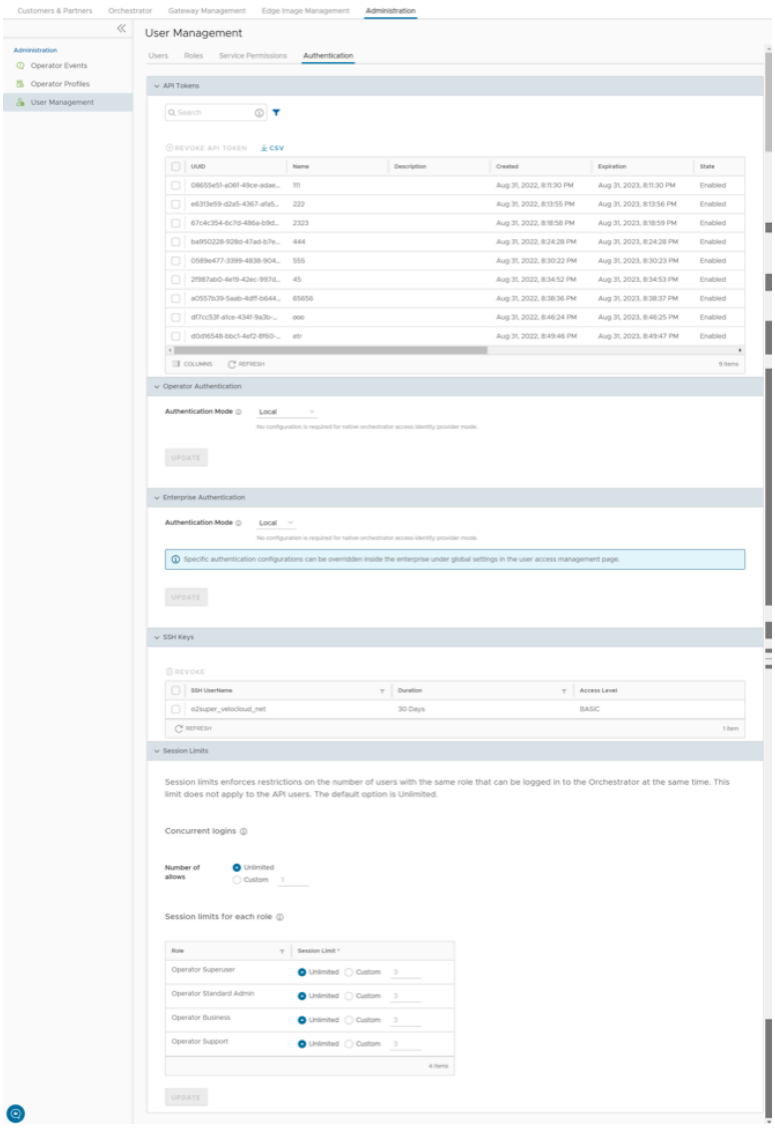
13.4 Authentication

The Authentication feature allows users to set the authentication modes for Operators and Enterprise users. Users can also view the existing API tokens.

To access the **Authentication** tab:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the left menu, select **User Management**, then choose the **Authentication** tab. The following screen appears:

Figure 13-12: Authentication-Operator



The various sections in the **Authentication** tab are explained below:

API Tokens

Users can access the Orchestrator APIs using token-based authentication, irrespective of the authentication mode. Operator Administrators with the right permissions can view the API tokens issued to Orchestrator users, including tokens issued to the Partner and Customer users. If required, an Operator Administrator can revoke the API tokens.

By default, the API Tokens are activated. To deactivate them, go to **Orchestrator** > **System Properties**, and set the value of the system property `session.options.enableApiTokenAuth` to **False**.

> **Note:** An Operator Superuser should manually delete inactive Identity Provider (IdP) users from the Orchestrator to prevent unauthorized access via API Token.

Configure the following options:

Table 45: API Tokens - Options and Descriptions

Option	Description
Search	Enter a search term to search for the matching text across the table. Use the advanced search option to refine the search results.
Revoke API Token	Select the token and select this option to revoke it. Only an Operator Super User or the user associated with an API token can revoke the token.
CSV	Select this option to download the complete list of API tokens in a .csv file format.
Columns	Selects the columns to be displayed or hidden on the page.
Refresh	Select to refresh the page to display the most current data.

An Operator Superuser can manage the API tokens for Enterprise users. For information on creating and downloading API tokens, see API Tokens.

Operator Authentication/Enterprise Authentication

Select one of the following Authentication modes: Local, Single Sign-On, or Radius.

- **Local:** This is the default option. Starting from the release 7.0.0, the **Local** authentication mode introduces a more secure two-factor authentication option: **TOTP**.

  > **Note:** Activating TOTP prevents users from switching back to the SMS option. For more information, see Time-Based One Time Passcode (TOTP).

- **Single Sign-On:** Operator users with Superuser permission can set up and configure Single Sign On (SSO) in Orchestrator. Single Sign-On (SSO) is a session and user authentication service that allows users to log in to multiple applications and websites with one set of credentials. Integrating an SSO service with Orchestrator enables the Orchestrator to authenticate users from an OpenID Connect (OIDC)-based Identity Providers (IdPs).

  > **Note:** Beginning in Release 6.1.0, the Orchestrator supports multiple IdPs, so a Partner on their Dedicated Orchestrator can configure an IdP independently of the VeloCloud SD-WAN TechOPS team. As a result, the Partner with Operator-level access can log in to their Dedicated Orchestrator using an integrated Single Sign-On service.

  Pre-requisites:

  - Users must have the Operator Superuser permission.

- Before setting up the SSO authentication in Orchestrator, users must set up Users, Service Permissions, and OpenID connect (OIDC) application for Orchestrator in the preferred identity provider's website.

Note:

- The **Single Sign-On** mode is available only for **Operator Authentication** in the Operator portal.
- Token-based authentication is deactivated for SSO users.

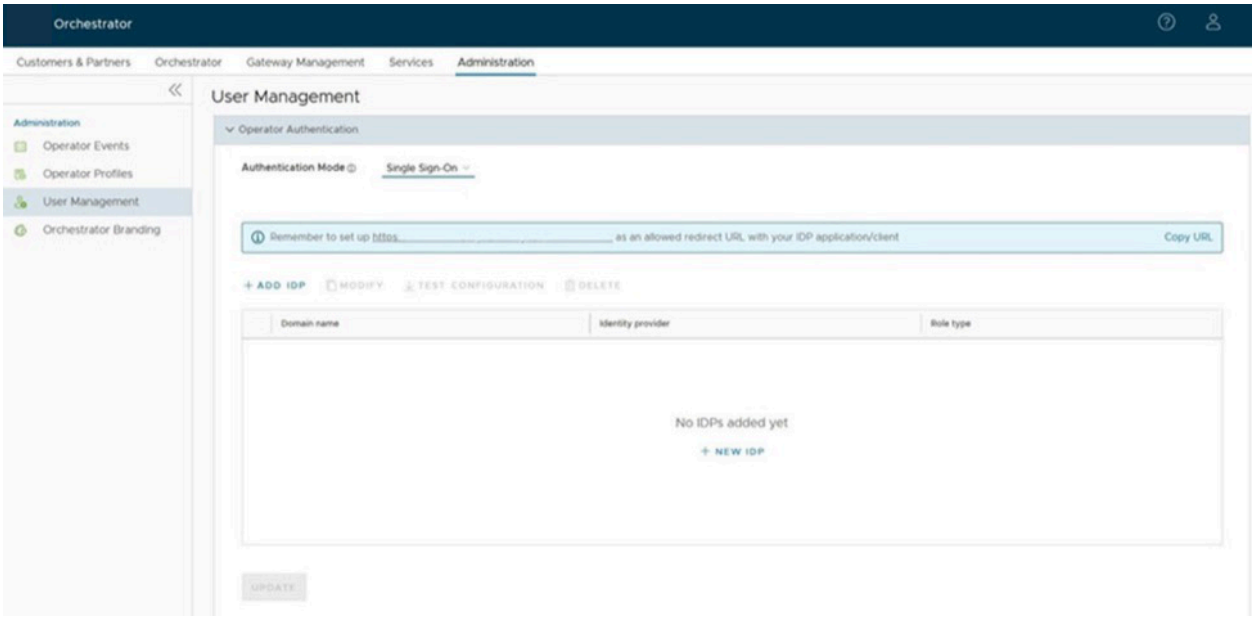
To enable Single Sign On (SSO) for Orchestrator, users must enter the Orchestrator application details into the Identity Provider (IdP). See the following topics in the *Arista VeloCloud SASE Global Settings Guide* for step-by-step instructions to configure the following supported IdPs:

- *Azure AD*
- *Okta*
- *OneLogin*
- *PingIdentity*

The Operator Authentication screen for Single Sign-On with Optional Multiple IdPs

With the new Multiple IdP feature in Release 6.1.0, the Single Sign-On screen changes from displaying one configuration screen for one Single Sign On account to displaying a table where multiple IdPs can be configured and tracked.

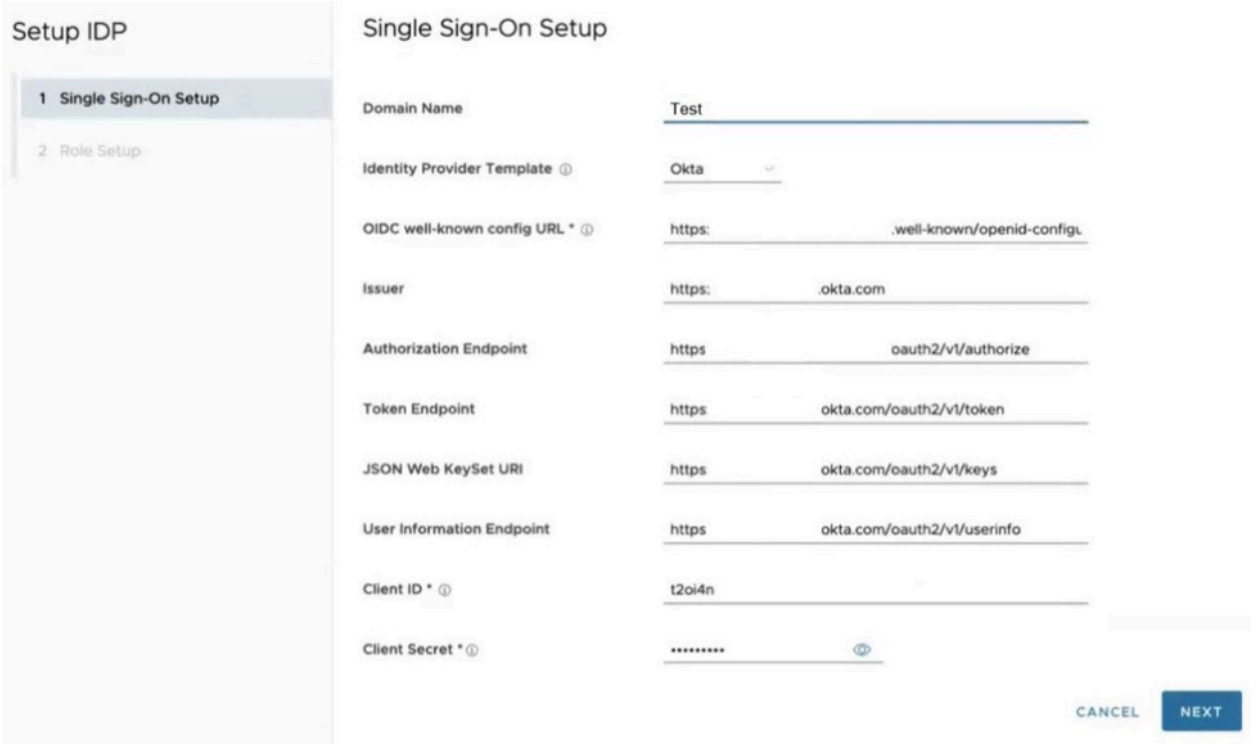
Figure 13-13: Configure Operator Authentication



With this new format, a Superuser Operator must select **+ NEW IDP** to add an IdP. Only then will the **Single Sign-On Setup** screen appear for configuring that particular IdP.

The workflow for configuring a Single Sign-On changes slightly with a user seeing two screens.

Figure 13-14: Single Sign-On Setup



On the **Single Sign-On Setup** screen, configure the following options:

Table 46: Single Sign-On Setup - Options and Descriptions

Option	Description
Identity Provider Template	From the drop-down menu, select your preferred Identity Provider (IdP) configured for Single Sign On. This populates fields specific to your IdP.
OIDC well-known config URL	Enter the OpenID Connect (OIDC) configuration URL for your IdP. For example, the URL format for Okta will be: https://{oauth-provider-url}/.well-known/openid-configuration.
Issuer	This field is auto-populated based on your selected IdP.
Authorization Endpoint	This field is auto-populated based on your selected IdP.
Token Endpoint	This field is auto-populated based on your selected IdP.
JSON Web KeySet URI	This field is auto-populated based on your selected IdP.
User Information Endpoint	This field is auto-populated based on your selected IdP.
Client ID	Enter the client identifier provided by your IdP.
Client Secret	Enter the client secret code provided by your IdP, that is used by the client to exchange an authorization code for a token.
Scopes	This field is auto-populated based on your selected IdP.

Once the **Single Sign-On Setup** is complete, the Operator needs to configure the **Role Setup** section.

Figure 13-15: Role Setup-Use Default Role

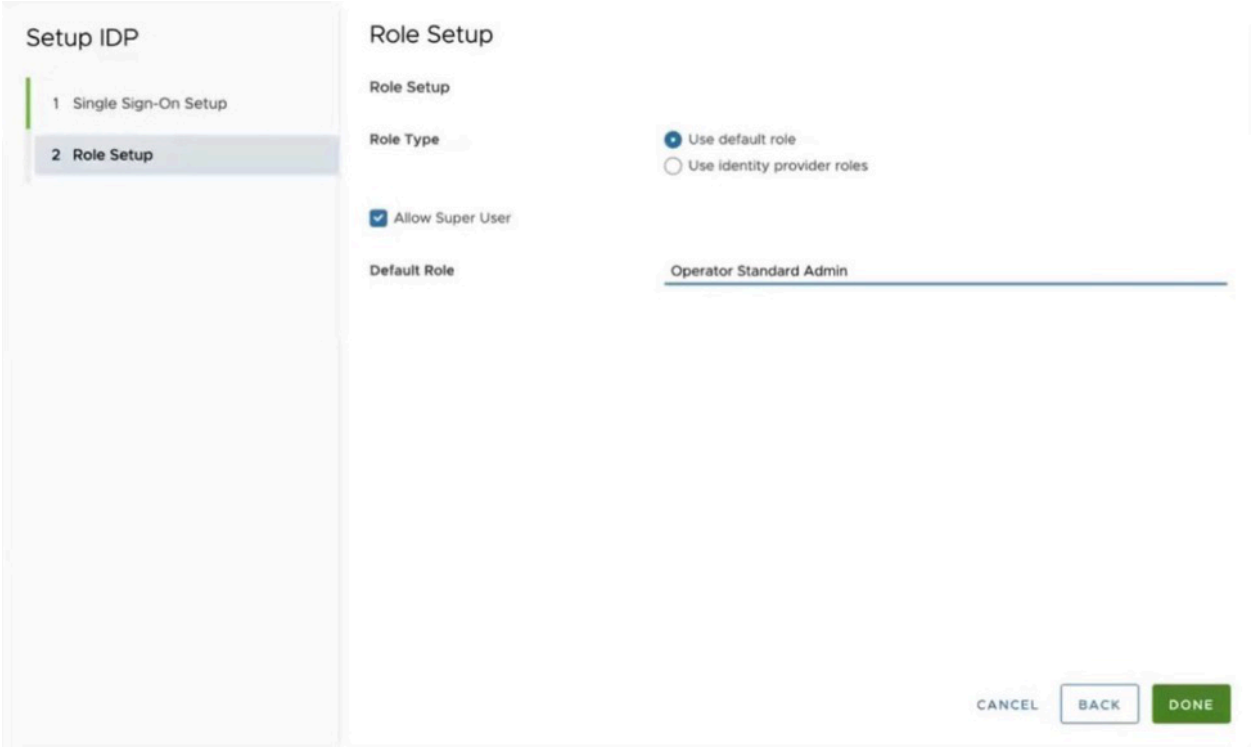
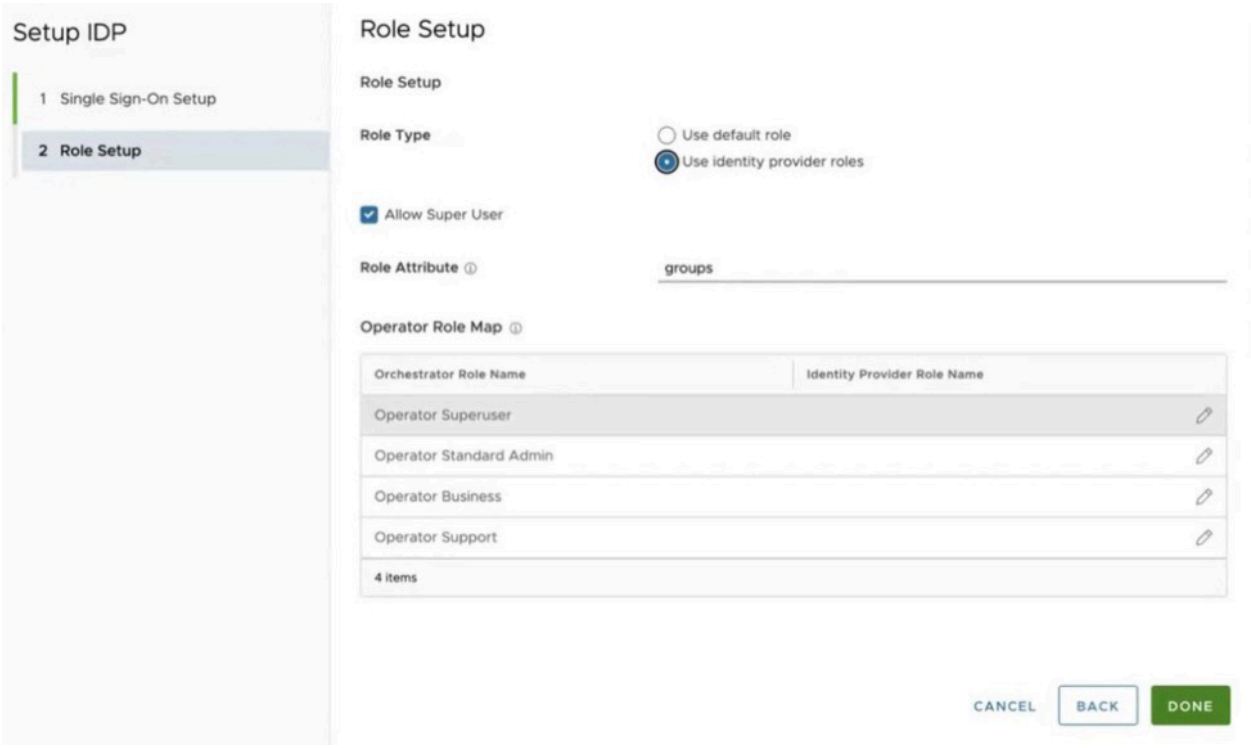


Figure 13-16: Role Setup-Use Identity Provider Roles (Default)



On the **Role Setup** screen, configure the following options.

Table 47: Role Setup - Options and Descriptions

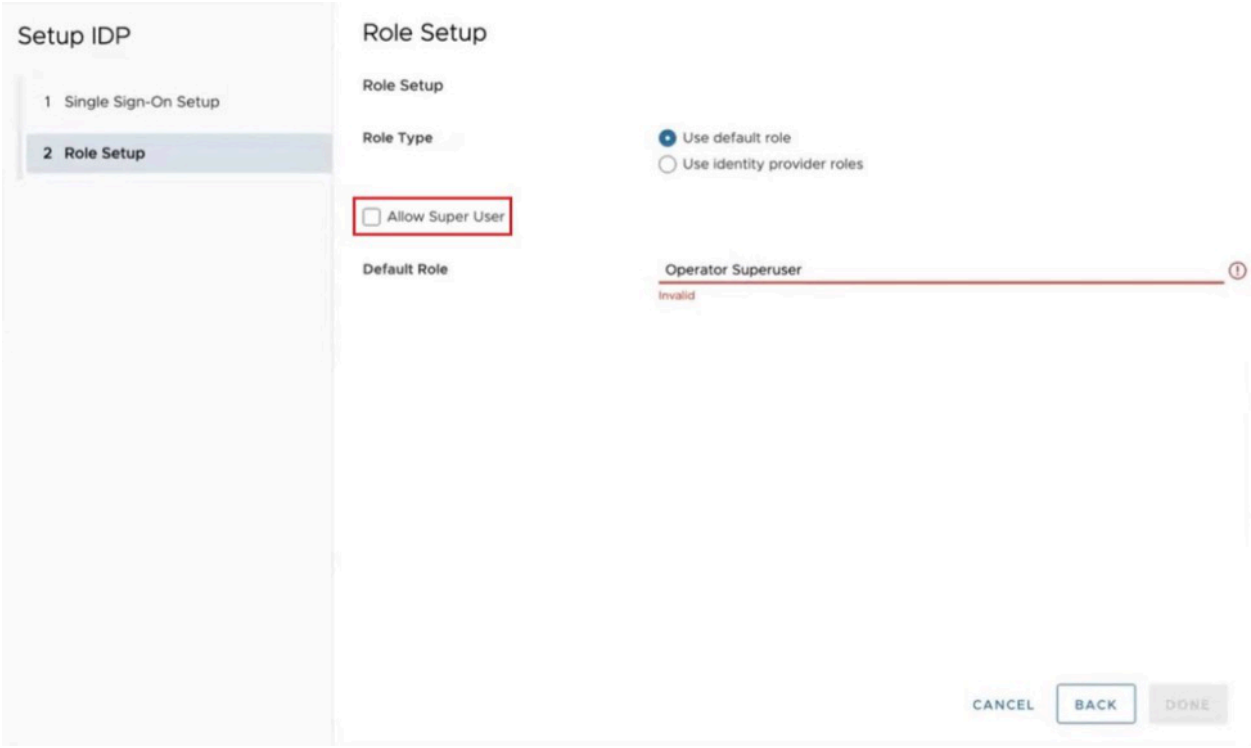
Option	Description
Role Type	Select one of the following two options: • Use default role • Use identity provider roles
Allow Super User	This option is for the Partner adding a second IdP. Unchecked this option as a Partner cannot have a Super User role on a Dedicated Orchestrator managed by Arista VeloCloud. In addition, remove the Super User role on the **Use identity provider roles** screen.
Role Attribute	Enter the name of the attribute set in the IdP to return roles.
Operator Role Map	Map the IdP-provided roles to each of the Operator user roles.

CAUTION: If configuring a second IdP for a Partner on an Orchestrator hosted by VeloCloud (Dedicated Orchestrator), the configuration must not include an Operator Superuser role.

Role Setup for a Partner-added second IdP where the **Allow Super User** checkbox is unchecked: This screen also shows that if users enter Operator Superuser as a default role, the Orchestrator displays

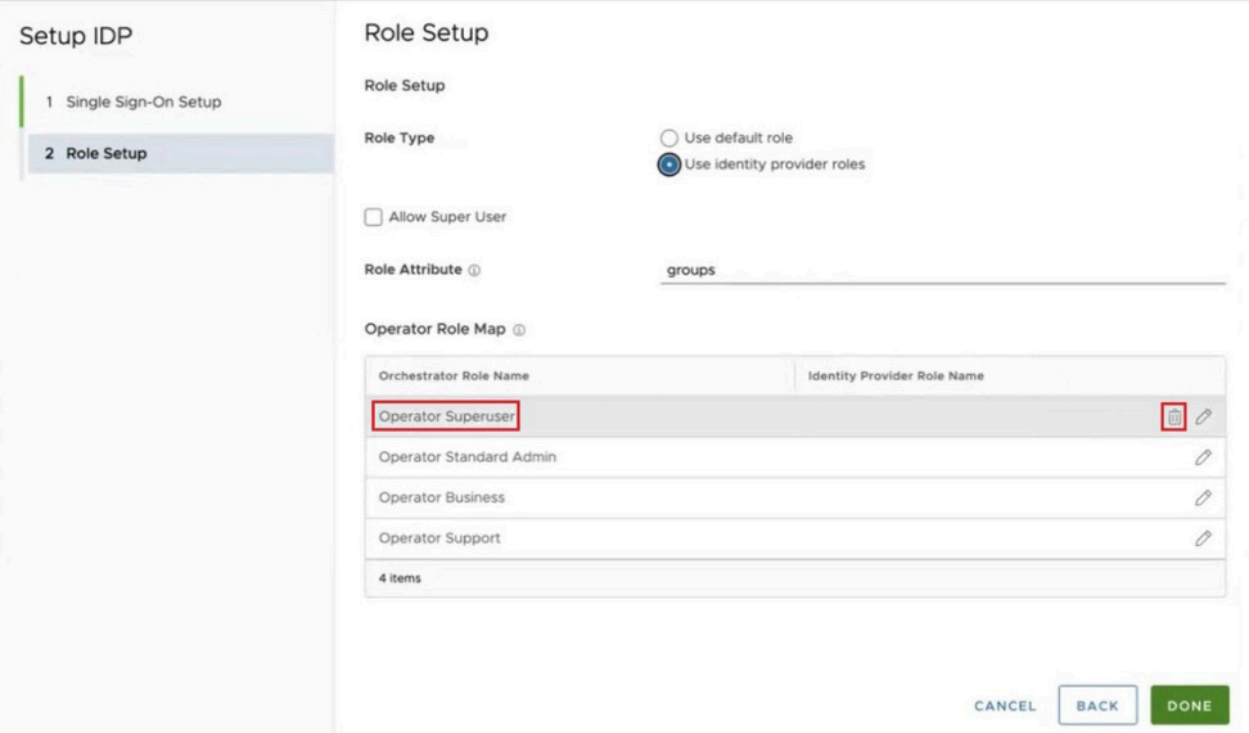
an error when that box is unchecked. The Default Role should be Operator Standard Admin for Partner Operator users.

Figure 13-17: Allow Super User



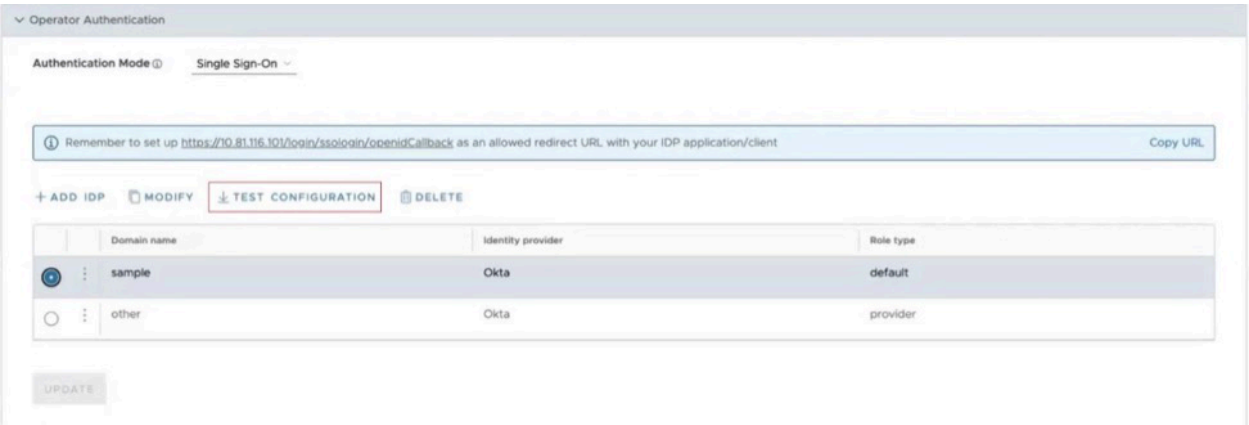
Role Setup for a Partner-added second IdP, where the Operator Superuser role must be removed.

Figure 13-18: Remove Operator Superuser Role



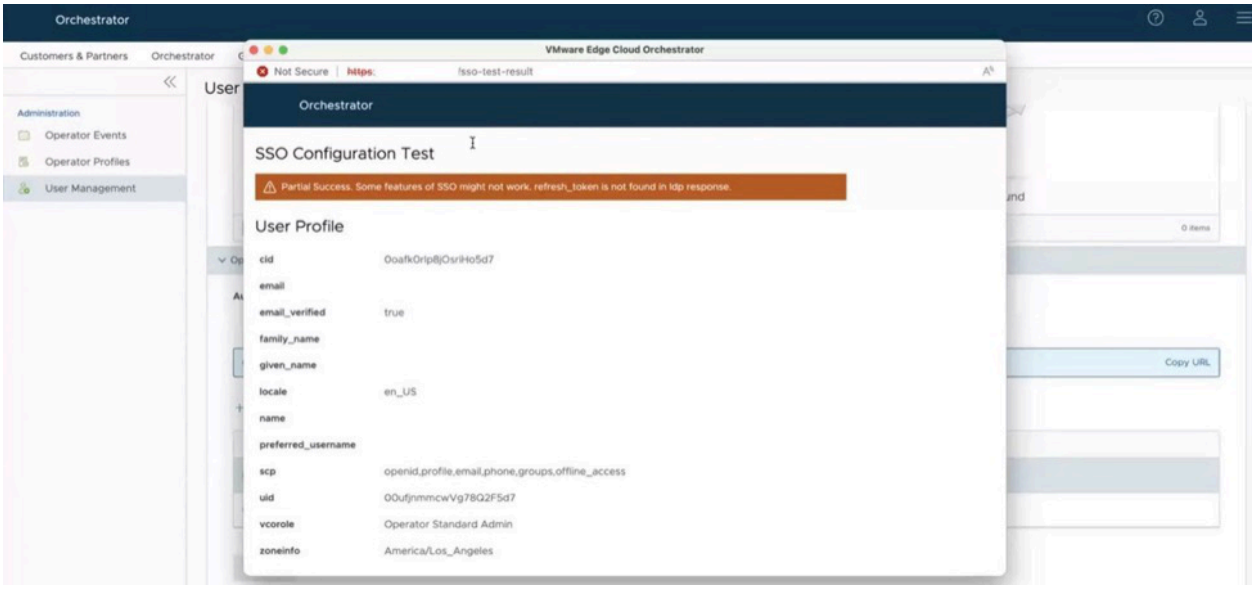
The Operator user can also test the configuration for a particular Single Sign-On/IdP configuration, by selecting the **Test Configuration** option

Figure 13-19: Test Configuration



Successful SSO Configuration Test: The "Partial Success" message only indicates this configuration does not have a refresh token configured. It is still a valid configuration.

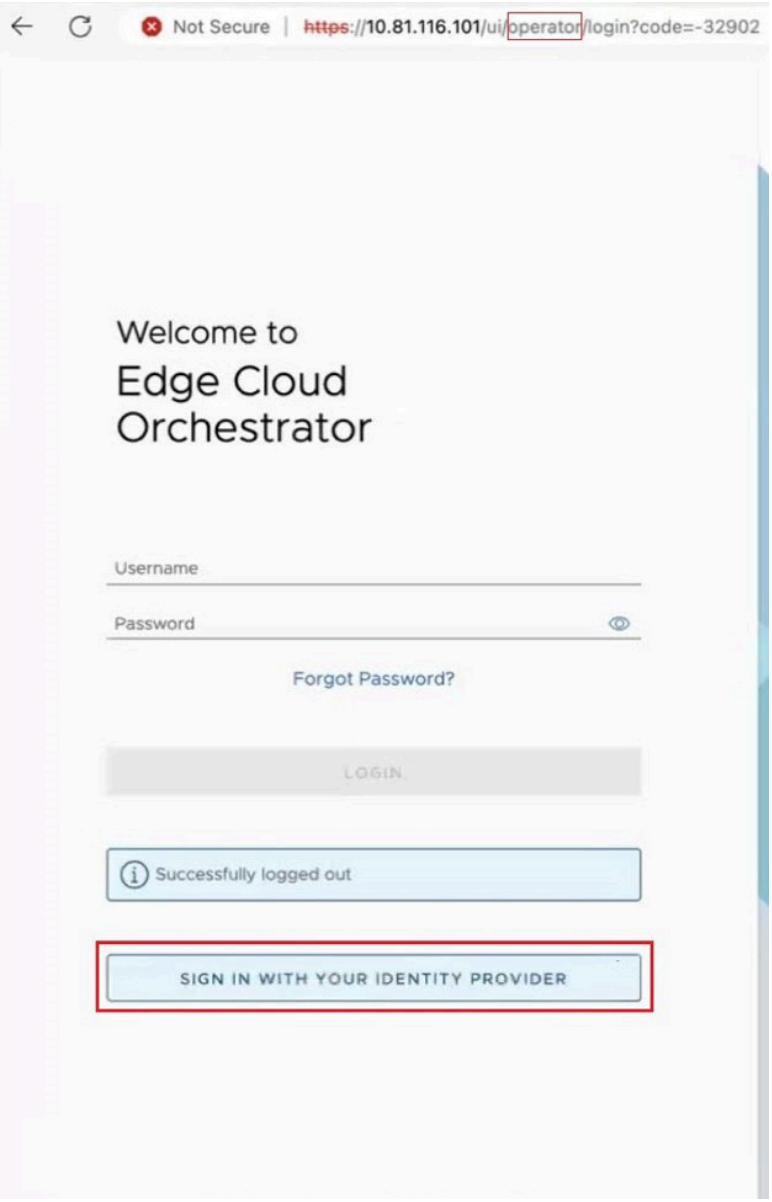
Figure 13-20: SSO Configuration Test



Logging in as a Partner with an Operator Role using your own IdP: A partner with an IdP configured can login to their Orchestrator by pulling up a browser and entering in the usual URL except they would add /operator to that URL. This pulls up the Operator login screen and includes a button **SIGN IN WITH YOUR IDENTITY PROVIDER**. On an Orchestrator with just one SSO IdP configured, selecting that button logs them in assuming the Operator user has the proper IdP credentials.

The Operator login screen has `/operator` in the URL and includes the 'Sign In With Your Identity Provider' button. Select this button to move on to the SSO screen.

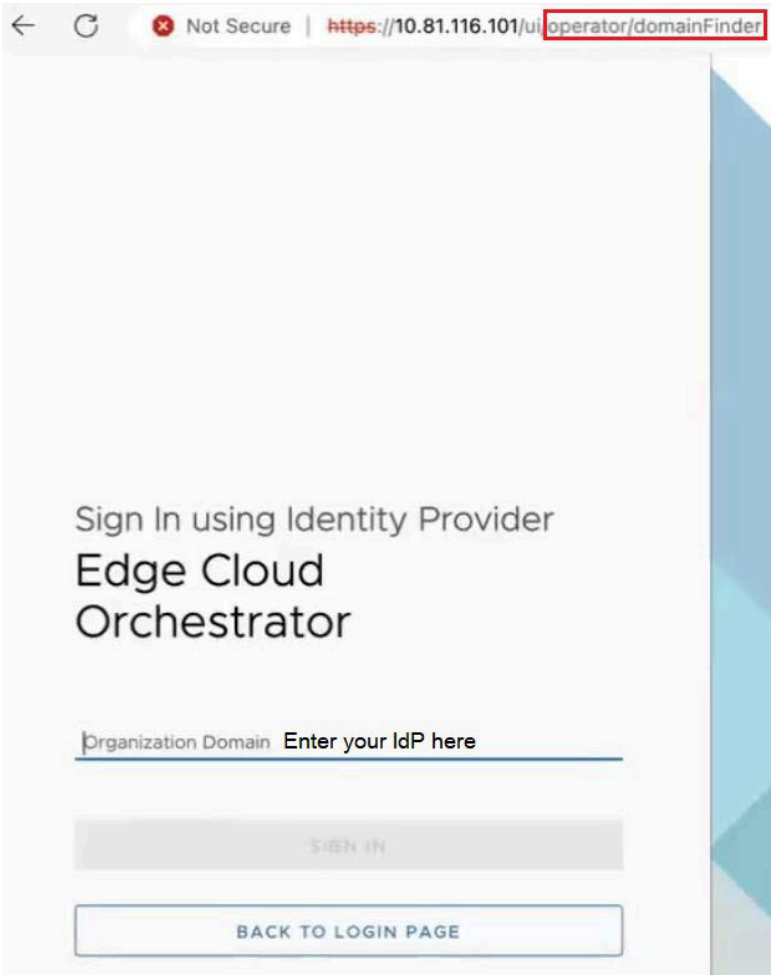
Figure 13-21: Orchestrator Operator Login Screen



On an Orchestrator with multiple IdPs configured, selecting that button takes users to a new screen for SSO sign-in. This is where the Partner Operator would enter in the **Domain Name** configured for the IdP. Once entered, select **Sign In** to log into the Orchestrator.

Where there are multiple IdPs configured, all users including the Partner are moved to this screen. The URL includes the text string `domainFinder`, but where it reads Organization Domain, enter your **Domain Name** for the IdP as configured earlier.

Figure 13-22: Sign In Using Identity Provider



Note: An easier method for a Partner using their own IdP is to bookmark the following their Orchestrator URL with this format: `https://orchestrator hostname` or `IP address/ui/operator/login?domain=IdP Domain Name`. This automatically takes users to the login screen and pre-populate the IdP Domain Name. For example for an Orchestrator with hostname `vco11-usor1.velocloud.net` where the IdP Domain Name is **Acme**, the Partner Operator could bookmark: `https://vco11-usor1.velocloud.net/ui/operator/login?domain=Acme` and when they selected that bookmark, the browser would still go to the Operator login screen. The difference is that now when they select **SIGN IN WITH YOUR IDENTITY PROVIDER**, the user is immediately logged in the Orchestrator with no extra step, as the domain is already provided in the URL.

For all configurations of an IdP, select **Update** to save the entered values. The SSO authentication setup is complete in the SD-WAN Orchestrator.

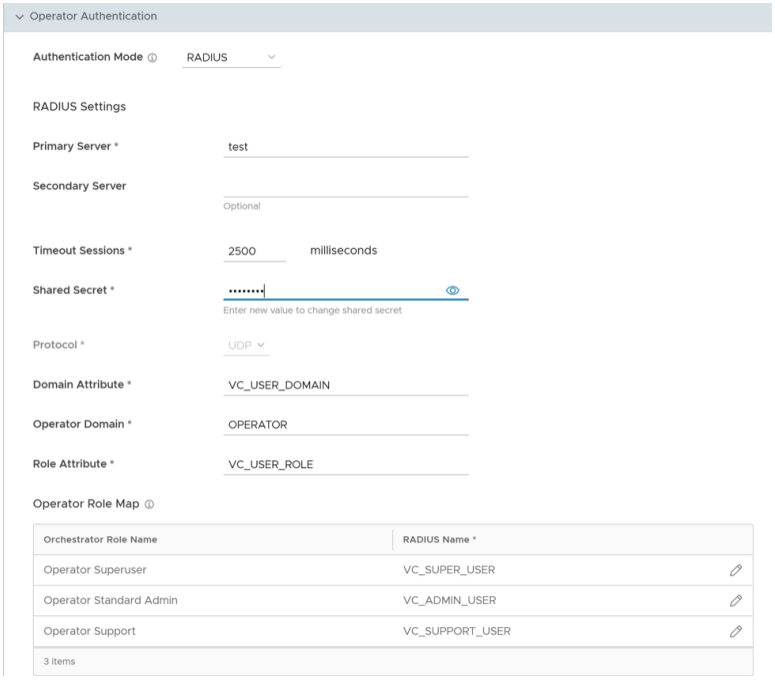
- **RADIUS**: Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol that enables remote access servers to communicate with a central server. RADIUS authentication provides a

centralized management for users. Configure the Orchestrator Authentication in RADIUS mode, so that the Operator and Enterprise Customers log into the portals using the RADIUS servers.

> **Note:** Copy the attributes required by the Radius server from the following directory: `/usr/share/node/node_modules/velocloud/lib/radius/raddb/dictionary.velocloud`. This file contains the necessary attributes, vendor name, and vendor ID.

To configure the Orchestrator Authentication in RADIUS mode, enter appropriate details in the following fields:

Figure 13-23: Configure Radius Authentication Mode



- Edit the **Protocol** value only in the **System Properties**. Navigate to **Orchestrator** > **System Properties**, and edit the protocol in the **Value** field of the system property `vco.operator.authentication.radius`.
- The **Operator Domain** field is available only for Operators.
- In the **Operator Role Map / Enterprise Role Map** section, map the RADIUS server attributes to each of the Operator or Enterprise user roles. This role mapping is used to determine the role users would be assigned when they log in to the Orchestrator using the RADIUS server for the first time.
- Select **Update** to save the entered values.

SSH Keys

Create only one SSH Key per user. Select the **User Information** icon located at the top right of the screen, then choose **My Account** > **SSH Keys** to create an SSH Key.

Operators can also revoke an SSH Key.

Select the **Refresh** option to refresh the section to display the most current data.

For additional information, see Configure User Account Details.

Session Limits

> **Note:** To view this section, an Operator user must navigate to **Orchestrator** > **System Properties**, and set the value of the system property `session.options.enableSessionTracking` to **True**.

The following are the options available in this section:

Table 48: Session Limits Option Descriptions

Option	Description
Concurrent logins	Allows setting a limit on concurrent logins per user. By default, **Unlimited** is selected, indicating that unlimited concurrent logins are allowed for the user.
Session limits for each role	Allows setting a limit on the number of concurrent sessions based on user role. By default, **Unlimited** is selected, indicating that unlimited sessions are allowed for the role. **Note:** The roles that are already created by the Operator on the **Roles** tab are displayed in this section.

Select **Update** to save the selected values.

13.4.1 Time-Based One Time Passcode (TOTP)

Release 7.0.0 introduces a new feature, the Time-based One-Time Passcode (TOTP) mechanism, for Two Factor Authentication (2FA). This feature replaces the current text-based 2FA mechanism (SMS) and mandates all future 2FA to use TOTP. Arista recommends selecting the TOTP authentication because it is more secure than the SMS-based authentication.

> **Note:** Only an Operator user can activate the TOTP feature for Partners and Customers.

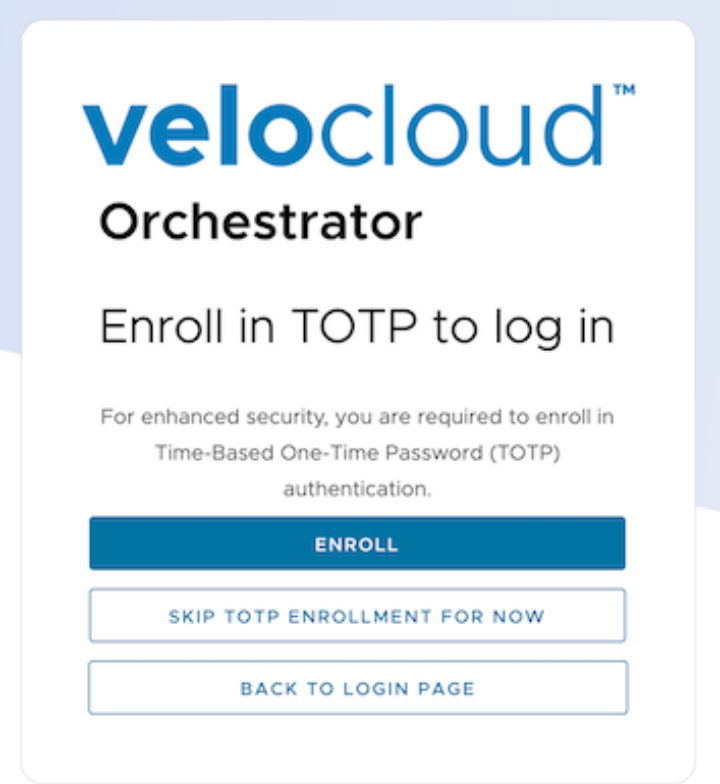
When a user enables TOTP under **User Management** > **Authentication**, the Orchestrator prompts all users who log in to either enroll (if not already enrolled) or provide the TOTP to complete authentication.

The procedure below explains the enrollment flow.

1. After enabling the TOTP, re-login to the VeloCloud Orchestrator.

The following screen appears if the user has not completed the TOTP enrollment.

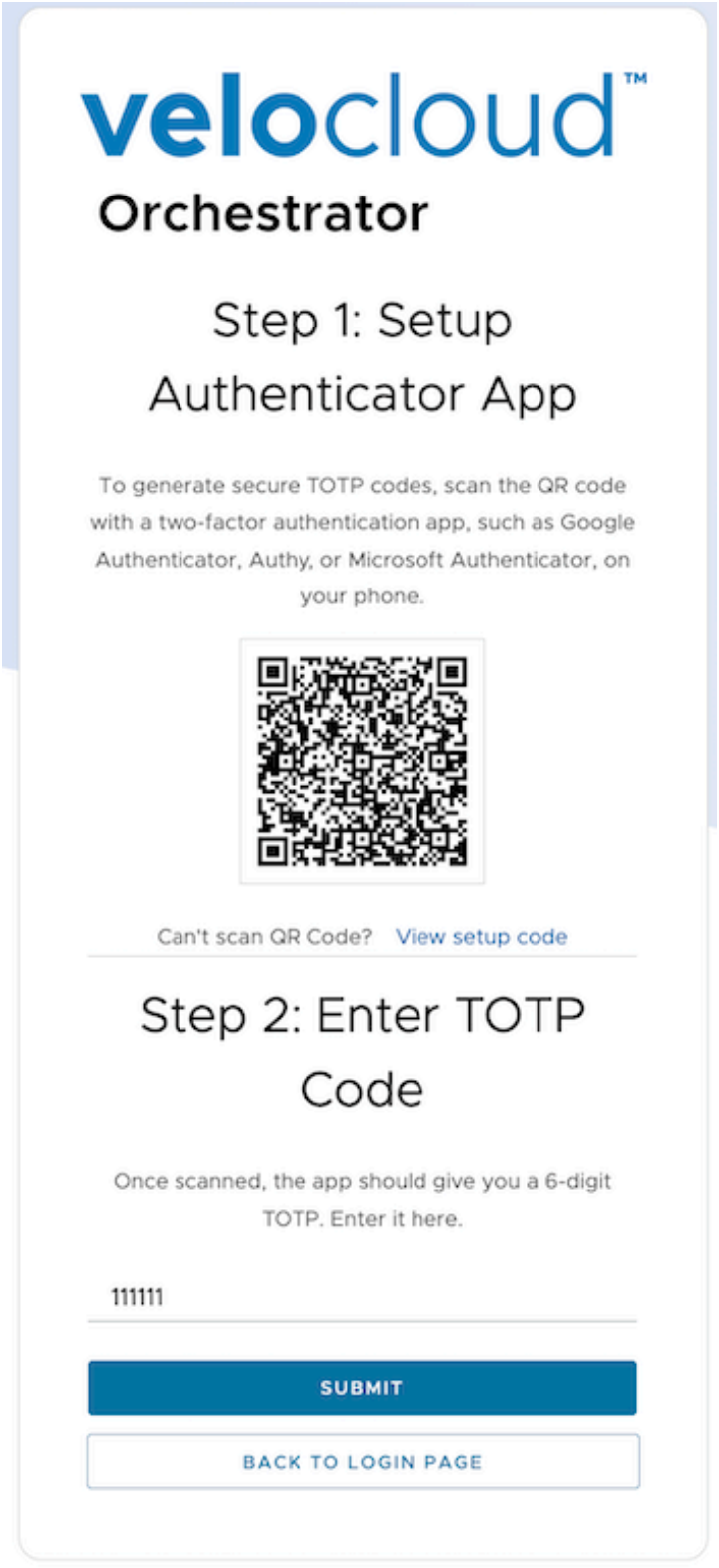
Figure 13-24: TOTP Enrollment



2. **Enroll**: Perform the below steps.
   a. Click **Enroll** to start the TOTP enrollment.
      The email address verification screen appears.
   b. After verifying the email address, enter the OTP sent to that email.

c. Select **Verify**.

Figure 13-25: Setup the Authenticator App



d. Scan the QR code using an authenticator application on your mobile phone.

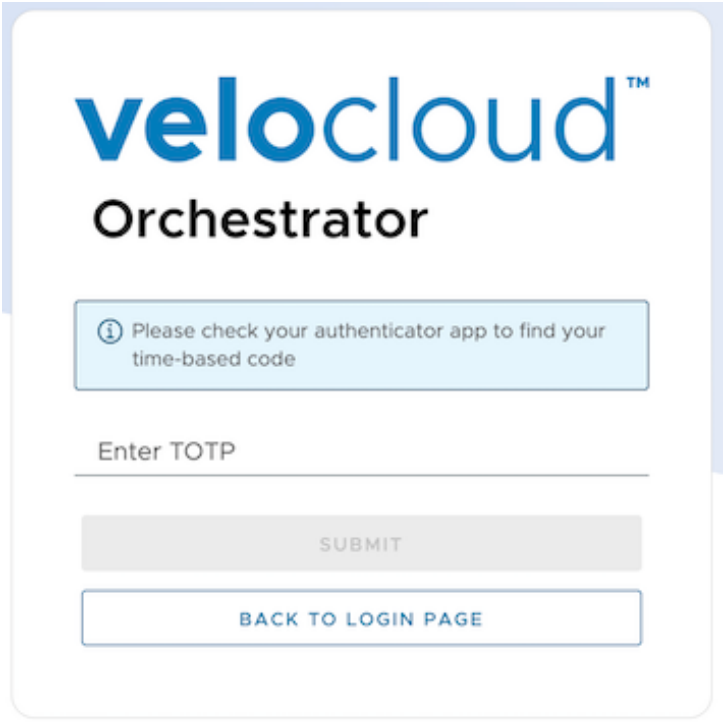
e. Enter the six digit TOTP, and then select **Submit**.
A success message appears on the screen.

f. Select the **Back To Login Page** button.

g. Enter the username and password, and select **Login**.

h. Enter the new TOTP generated on the authenticator application, and then select **Submit**.

Figure 13-26: Enter TOTP Details



Note: The Authenticator application generates a new TOTP every 30 seconds.

3. Click **Skip TOTP Enrollment for now** to skip the enrollment temporarily. This option appears only when the **Require two factor authentication for Login** checkbox under the **User Management** > **Authentication** > **User Authentication** section remains clear.
4. Click **Back to Login Page** to go to the user login page.

Resetting a TOTP

Users can reset TOTP from the **My Account** page.

1. On the User Information panel, click **My Account**.
2. In the **Profile** tab, select the **Reset TOTP Enrollment** button.

Note: Changing the account password causes the TOTP reset. However, resetting TOTP does not require changing the password.

For more information, see Configure User Account Details.

Chapter 14

Orchestrator Branding for Operator

This section provides guidelines to customize the Orchestrator user interface (UI) to your company's brand. As an Operator user, you can brand the Orchestrator UI by applying your company's name, logo, and colors at a global level.

Note: Orchestrator Branding applies only to dedicated Orchestrator instances. For shared Orchestrator instances, the branding feature is not available.

To enable Operator users to customize the orchestrator UI branding at a global level, you must first activate the **Operator only Branding** feature. To activate **Operator only Branding**, in the **Operator** portal, go to **Orchestrator** > **System Properties**, and set the value of the system property `operator.branding.enabled` to **True**.

Note: Changing the `operator.branding.enabled` property to true will immediately override any Partner/Enterprise branding, even if the Operator branding is unchanged.

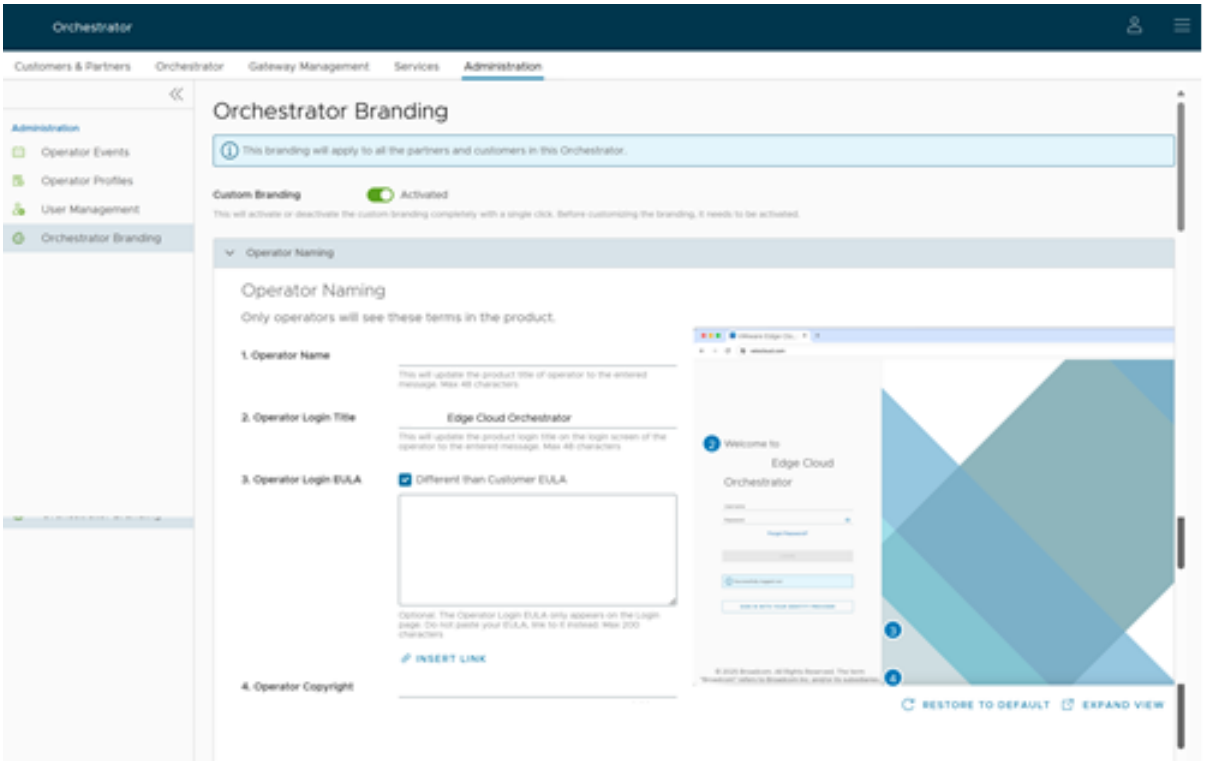
Note: By default, this system property is set to **False**, allowing Partner and Enterprise users to customize the Orchestrator UI branding for their Orchestrator instances at the Partner and Enterprise levels, respectively.

As an Operator user, to customize the branding at a global level for all the Partners and Enterprises in the Orchestrator, perform the following steps:

1. In the **Operator** portal, select **Administration** from the top menu.
2. From the **left** menu, choose **Orchestrator Branding**.

The **Orchestrator Branding** page appears.

Figure 14-1: Orchestrator Branding



3. To customize branding, activate the **Custom Branding** feature by turning **on** the **Custom Branding** toggle button.
4. You can customize the following branding aspects of the Orchestrator UI:
   a. Operator Naming
   b. General Product Naming
   c. Support Naming
   d. Logos
   e. Header Display Name and Color
5. As you customize the branding, the changes are applied to the Preview image on the right. Select **Expand View** to expand the preview image. Select **Restore to Default** to restore the branding settings to default.
6. Once you are done with branding customization, select **Save Changes** and refresh the Orchestrator to view the applied custom branding.

> **Note:** The branding will apply to all the Partners and Enterprises in the Orchestrator.

7. To deactivate the **Custom Branding** feature, turn off the **Custom Branding** toggle button.
   All branding settings will be restored to their default values.

Operator Naming Branding

You can customize the following textual elements located on the Operator Login screen.

Table 49: Customized Element Descriptions

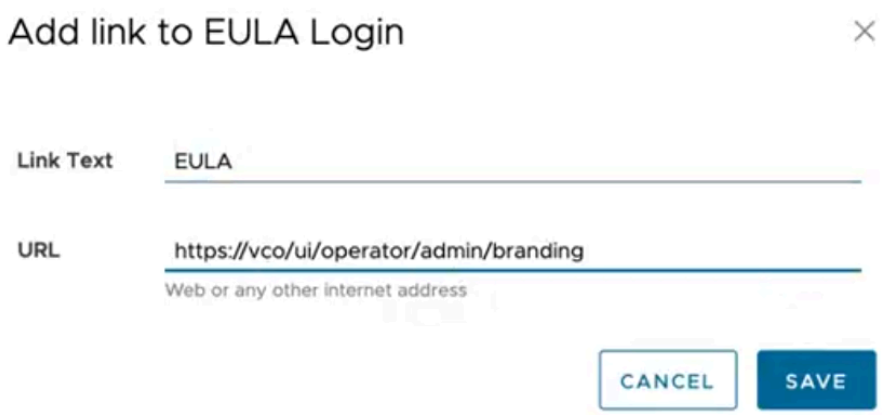
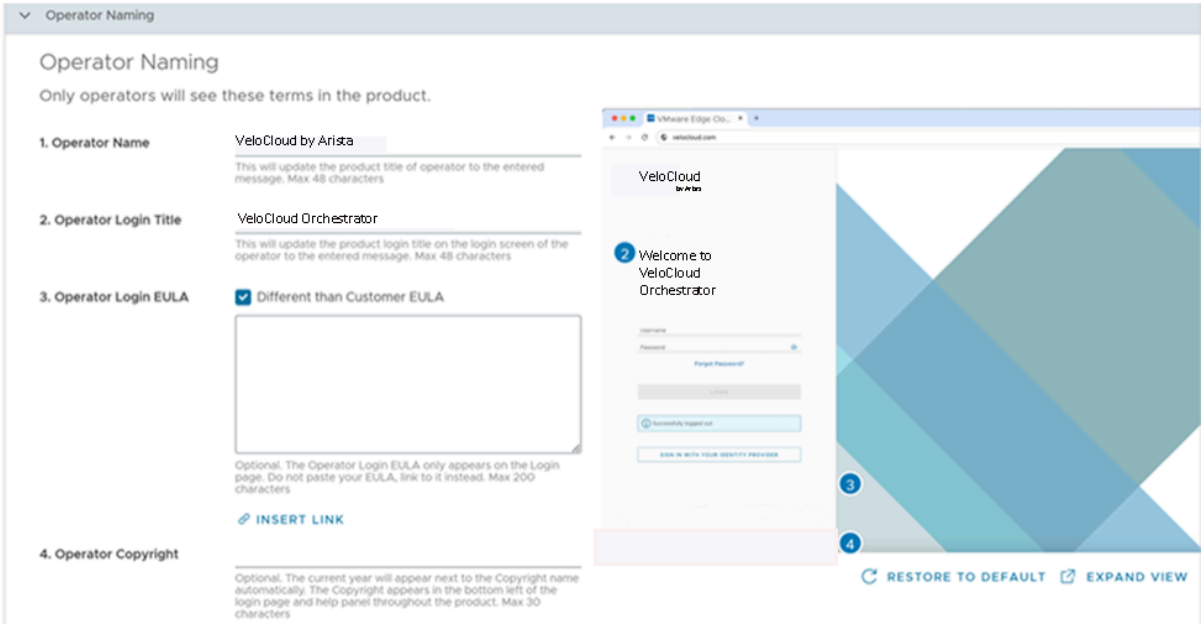
Element	Description
Operator Name	Enter your Operator name. This updates the product title of Operator to the entered text. The Operator name is a maximum of 48 characters.
Operator Login Title	Enter your Operator login title. This updates the product login title on the login screen of the Operator to the entered text. The Operator login title is a maximum of 48 characters.
Operator Login EULA	This is optional. Add your Operator login EULA, limited to 200 characters. The Operator login EULA only appears on the login screen. You can either enter your EULA in the box and then add a link by selecting the EULA, or directly add a link to the EULA login by choosing **Insert Link**. **Figure 14-2: Add Link to EULA Login** 
Operator Copyright	This is optional. Enter your Operator copyright name and text. The current year will appear next to the copyright name automatically. The copyright appears in the bottom left of the login page and help panel throughout the product. The Operator copyright text is a maximum of 30 characters. If you have not entered any customized copyright text, the default copyright will be displayed.

Figure 14-3: Operator Naming



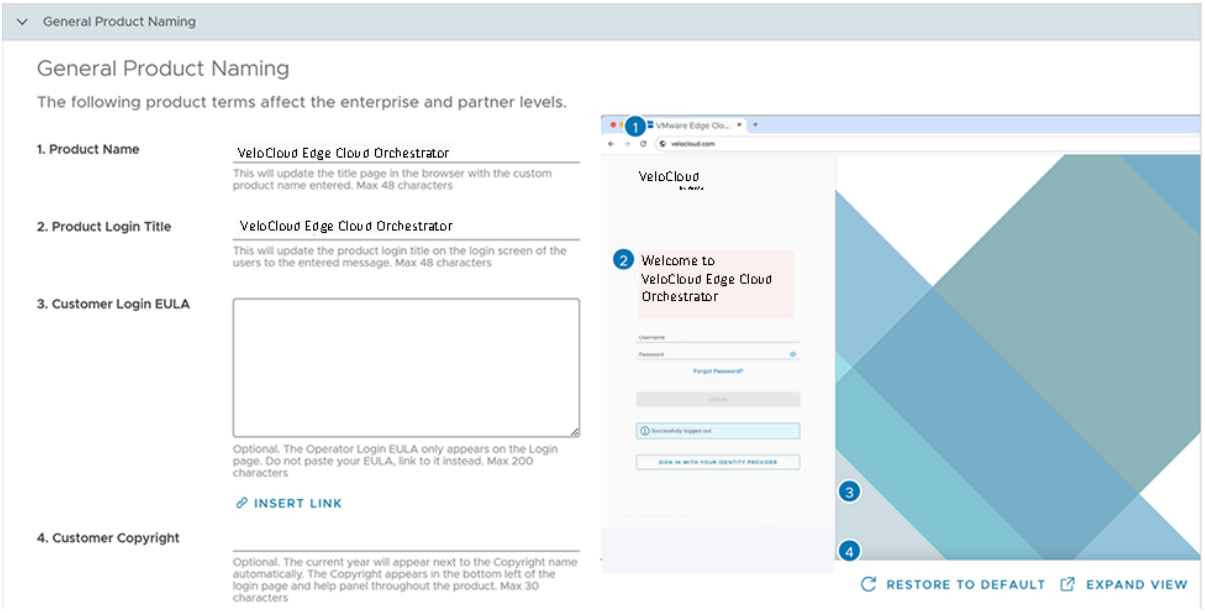
General Product Naming Branding

You can customize the following textual elements located on the Partner and Enterprise Login screen.

Table 50: General Product Element Descriptions

Element	Description
Product Name	Enter your product name. This updates the title page in the browser with the custom product name entered. The product name can be a maximum of 48 characters.
Product Login Title	Enter your product login title. This updates the product login title on the login screen of the users to the entered text. The product login title can be a maximum of 48 characters.
Customer Login EULA	This is optional. Add your Customer login EULA, limited to 200 characters. The Customer login EULA only appears on the login screen. You can either enter your EULA in the box and then add a link by selecting the EULA, or directly add a link to the EULA login by selecting **Insert Link**.
Customer Copyright	This is optional. Enter your Customer copyright name and text. The current year will appear next to the copyright name automatically. The copyright appears in the bottom left of the Customer login page and help panel throughout the product. The Customer copyright text is a maximum of 30 characters. If you have not entered any customized copyright text, the default copyright will be displayed.

Figure 14-4: General Product Naming



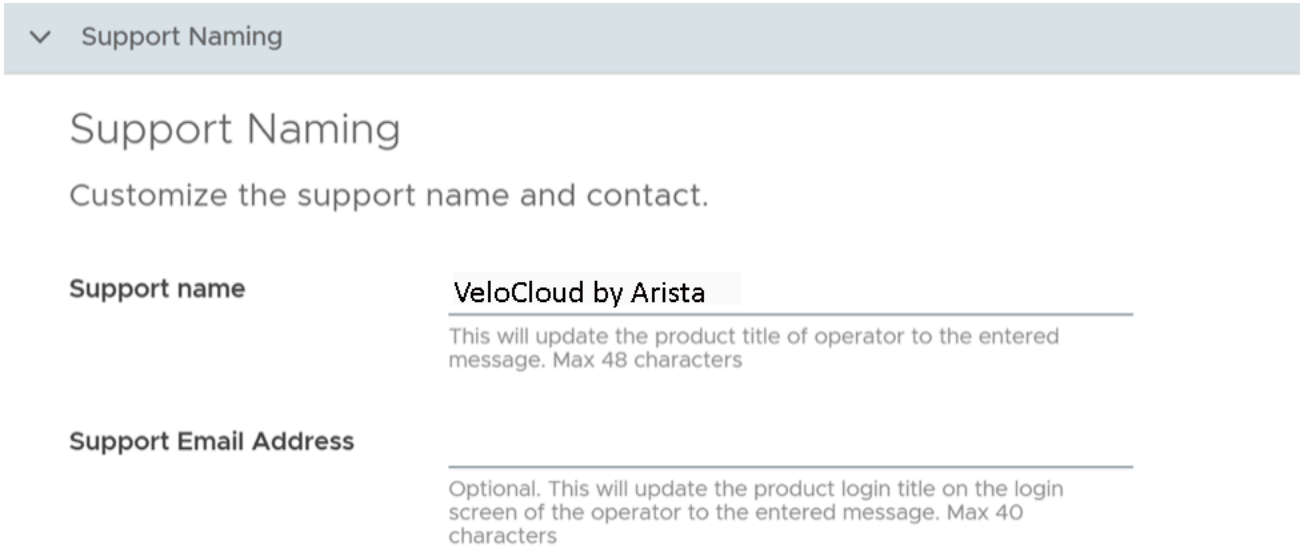
Support Naming Branding

You can customize the Support name and contact details.

Table 51: Support Name Element Descriptions

Element	Description
Support Name	Enter your custom support name. This updates the product title of Operator to the entered text. The support name is a maximum of 48 characters.
Support Email Address	This is optional. Enter your custom support email address. This updates the product login title on the login screen of the Operator to the entered text. The support email address is a maximum of 40 characters.

Figure 14-5: Support Naming



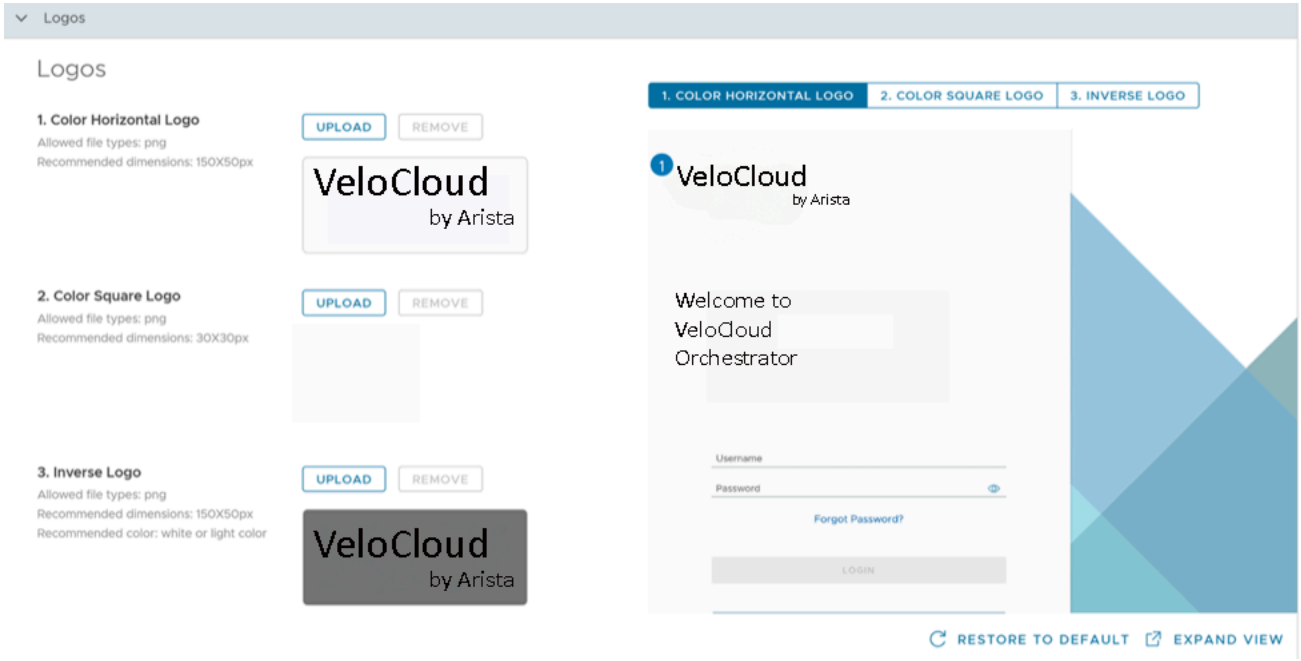
Logos Branding

Your logo is displayed on the top, left corner of the Login page of the Orchestrator UI. You can customize the following logo elements.

Table 52: Logo Branding Element Descriptions

Element	Description
Color Horizontal Logo	Select and upload your custom horizontal logo by selecting **Upload**. Adhere to the following Logo requirements: • Allowed file types: png • Recommended dimensions: 150X50px
Color Square Logo	Select and upload your custom square logo by selecting **Upload**. Adhere to the following Logo requirements: • Allowed file types: png • Recommended dimensions: 30X30px
Inverse Logo	Select and upload your custom inverse logo by selecting **Upload**. Adhere to the following Logo requirements: • Allowed file types: png • Recommended dimensions: 150X50px • Recommended color: white or light color

Figure 14-6: Logo Branding



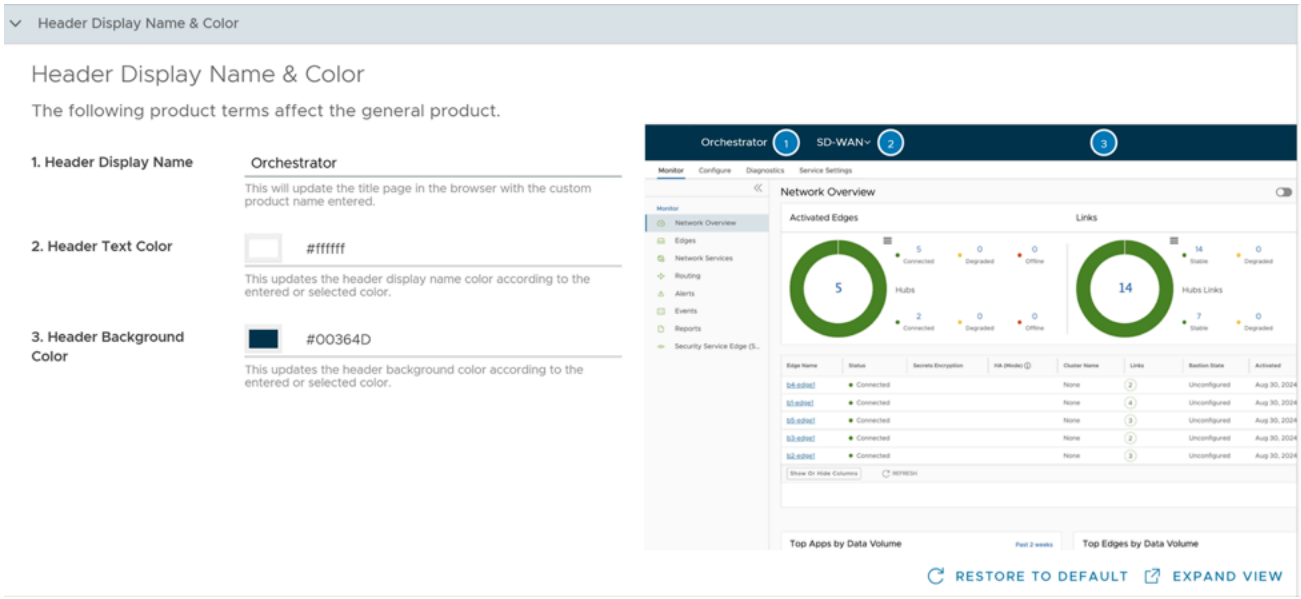
Header Display Name and Color Branding

You can customize the following textual and visual elements located on the Orchestrator UI header.

Table 53: Header Display Name and Color Branding Element Descriptions

Element	Description
Header Display Name	Enter your header display name. This updates the title page in the browser with the custom product name entered.
Header Text Color	Enter or select the header text color. This updates the header display name color according to the entered or selected color.
Header Background Color	Enter or select the header background color. This updates the header background color according to the entered or selected color.

Figure 14-7: Header Display Name and Color



Chapter 15

Manage User Agreements

Orchestrator allows an Operator Super User and Operator Standard Administrator to create and manage End User License Agreements. Only an Operator Super User can create an End User License Agreement.

1. In the **Operator** portal, select the **Administration** tab, then, and the left pane, choose the **User Agreements** button.
2. By default, the User Agreement option is deactivated. To activate this option, navigate to the **System Properties** in the Operator portal, and set the value of the System Property `session.options.enableUserAgreements` as **True**.

   In addition, you can configure the display mode of the User Agreement by defining the Value of the System Property `vco.enterprise.userAgreement.display.mode` as follows:

   - **NONE** — The User Agreement is not displayed to any of the Enterprise Users. This is the default value.
   - **ALL** — The User Agreement is displayed to all the Enterprise Users.
   - **WITH_MSPS** — The User Agreement is displayed to all the Enterprise Users with MSPS.
   - **WITHOUT_MSPS** —The User Agreement is displayed to all the Enterprise Users without MSPS.

     The above display settings apply to all Customers managed by the Operator. As an Operator, you can override these settings for each Enterprise Customer, as described in Configure Customers. Only an Enterprise Super User or Partner Super User can accept a license agreement, based on the System Property settings.

   Once the properties mentioned earlier are set, the **User Agreement** page appears on the **Administration** tab.
3. To create and manage a **User Agreement**, select **Administration** > **User Agreements** tab in the Operator portal and perform the following actions:

Table 54: User Agreement Option Descriptions

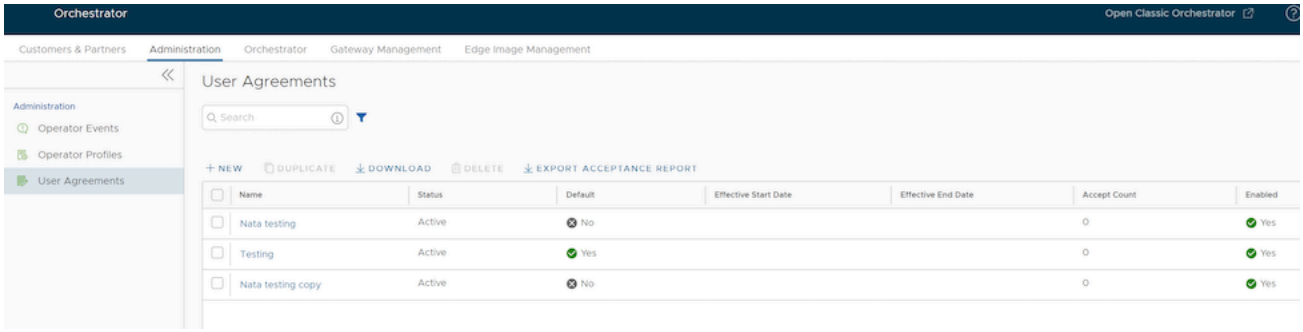
Option	Description
New	Creates a new End User License Agreement.
Duplicate	Duplicates and creates a copy of the selected User Agreement.
Download	Downloads a copy of the User Agreement details.
Delete	Deletes the selected User Agreements.
Export Acceptance Report	Exports a report of all the customers who have accepted the User Agreements to a CSV file.

Note: To **Update**, select the existing agreement in the table and update as required.

Create a User Agreement

Only Operator Super Users and Operator Standard Administrators can create a new user agreement. You can create multiple active user agreements and set the default one from the list. You can also choose and configure the active user agreement you want to display for a particular customer.

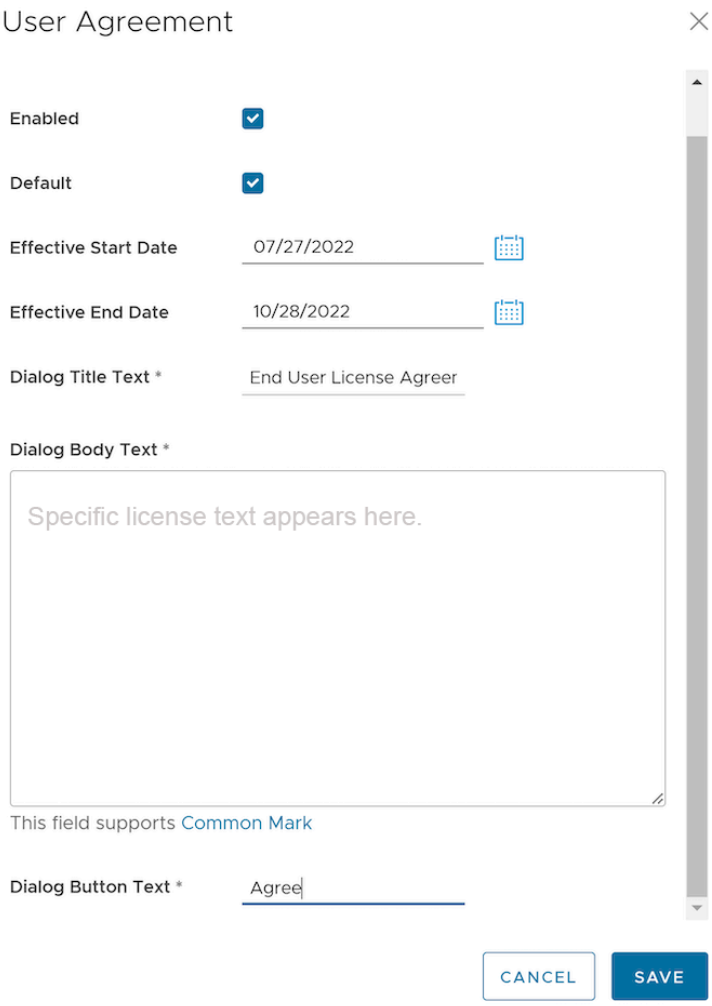
Figure 15-1: Manage User Agreements



- On the **Administration** tab, choose **User Agreements** and select **New**.

  The **User Agreement** dialog box appears.

- Enter the following information in the **User Agreement** dialog box:
- **Figure 15-2: Create User Agreement - Agree**



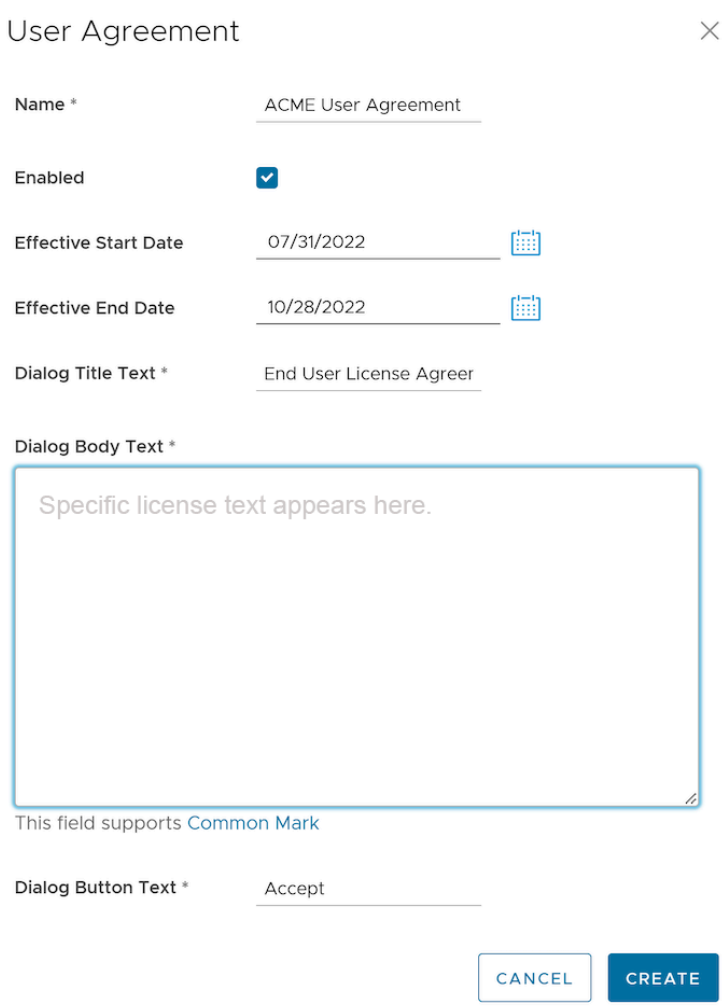
- **Table 55: User Agreement Option Descriptions**

Option	Description
Name	Enter the name for the user agreement.
Enabled	By default, this check box is selected. If unselected, the user agreement is Inactive.
Effective Start Date	Enter the date from which the user agreement is effective.
Effective End Date	Enter the date until which the user agreement is effective.
Dialog Title Text	Enter a title for the user agreement.
Dialog Body Text	Enter the descriptive user agreement text that would be visible to the Customer.
Dialog Button Text	Enter the text to be displayed on the button that the customer would select to accept the agreement.

- Select **Create**.

The agreements display on the **User Agreements** page.

Figure 15-3: Create User Agreement - Accept



- Select an inactive agreement, then select **Delete**, to delete it.

> **Note:** Active agreements cannot be deleted.

When an Enterprise Super User or Partner Super User logs into the Orchestrator for the first time, a **User Agreement** message pops up prompting the user to accept the agreement. The user must accept the agreement to get access to the Orchestrator. If the user does not accept the agreement, they get automatically logged out.

Chapter 16

Manage Gateway Pools and Gateways

The network consists of multiple service Gateways deployed at the top-tier network and cloud data centers. The Gateway provides the advantage of cloud-delivered services and optimized paths to all applications, branches, and data centers. Service providers can also deploy their Partner Gateways in their private cloud infrastructure.

This topic contains the following sections:

- Manage Gateway Pools
- Manage Gateways
- VeloCloud Gateway Migration
- Diagnostic Bundles for Gateways

16.1 Manage Gateway Pools

A Gateway Pool is a logical grouping of multiple Gateways. Users can organize Gateways into these pools and then assign them to specific networks to provide scalable and redundant access points for Edges.

Gateways can be organized into pools that are then assigned to a network. An unpopulated default Gateway pool is available after users install Orchestrator. If required, users can create additional Gateway pools.

As an Operator Super user and Operator Admin user, users can create, clone, manage, download, and delete Gateway pools created by both Operator and Partner users.

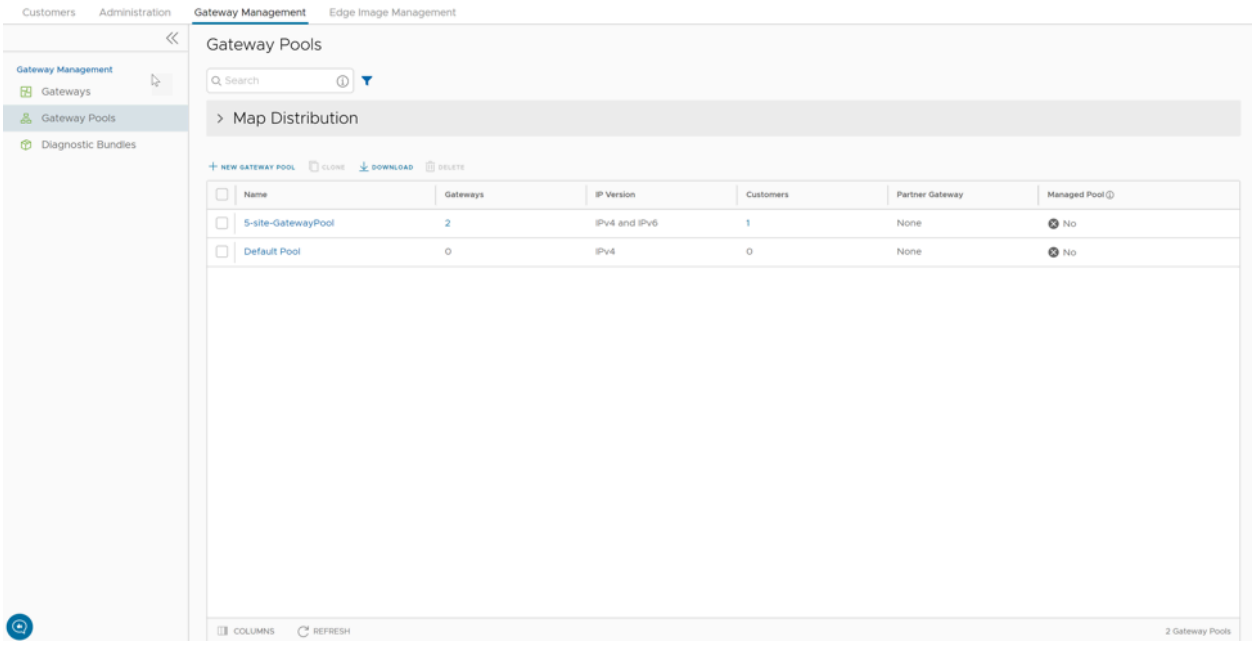
Note: The Operator Business Specialist user and the Operator IT support user can only view the configured Gateway pools and download the CSV file.

To manage Gateway pools, perform the following steps:

1. Log in to the **Orchestrator** as an Operator Super user or Admin user.
2. In the Orchestrator UI, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane.

The **Gateway Pools** page appears.

Figure 16-1: Manage Gateway Pools



3. To search a specific Gateway pool, enter a relevant search text in the **Search** box. For advanced search, select the **filter** icon next to the **Search** box to filter the results by specific criteria.
4. The **Map Distribution** section displays the Gateways on a map. The user can click the **+** and **-** buttons to zoom in and zoom out the map, respectively. In the **Gateway Pools** table, if users have selected any Gateway pools, then only the Gateways in the selected pools are displayed on the map. Otherwise, all Gateways are displayed on the map.

   The **Gateway Pools** table displays the existing Gateway pools with the following details.

Table 56: Gateway Pools Field Descriptions

Field	Description
Name	Specifies the name of the Gateway pool. When selecting on a Gateway pool link in the **Name** column, the user gets redirected to the **Gateway Pools Overview** page.
Gateways	Specifies the number of Gateways available in the Gateway pool. When selecting a Gateway link in the **Gateways** column, the user gets redirected to the **Gateway Overview** page.
IP Version	Specifies whether the Gateway Pool utilizes an IPv4 address only or supports a dual-stack configuration with both IPv4 and IPv6 addresses. **Note:** When assigning Gateways to the Gateway pool, ensure that the IP address type of the Gateway matches the IP address type of the pool.
Customers	Specifies the number of Enterprise Customers associated with the Gateway pool. When selecting a Customer link in the **Customers** column, a dialog opens with the listed customers. If a user selects a customer, then the UI redirects the user to the **Configure Customer** page.
Partner Gateway	Specifies the Partner Gateway's status. The following are the available options: • **None** - Use this option when Enterprises assigned to this Gateway pool do not require Gateway Partner handoffs. • **Allow** - Use this option when the Gateway pool must support both Partner Gateways and Cloud Gateways. • **Only** (Partner Gateways) - Use this option when Edges in the Enterprise should not be assigned Cloud Gateways from the Gateway pool, but can select only the Gateway-1 and Gateway-2 set for the individual Edge.
Managed Pool	Specifies if a Partner can manage the Gateway pool.

On the **Gateway Pools** page, users can perform the following activities:

- **New Gateway Pool** - Creates a new Gateway pool. See Create New Gateway Pool.
- **Clone** - Creates a new Gateway pool by cloning the existing configurations from the selected Gateway pool. See Clone a Gateway Pool.
- **Download** - Downloads the CSV file for all Gateway pools or the selected Gateway pool.
- **Delete** - Deletes the selected Gateway pool. Users cannot delete a Gateway pool that a Partner or an Enterprise Customer is already using.
- Users can also configure the existing Gateway pools by selecting the name link of the Gateway pool. See Configure Gateways.

16.1.1 Create New Gateway Pool

In addition to the default Gateway pool, users can create new Gateway pools and associate them with Enterprise Customers.

1. In the **Orchestrator UI**, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane.

The **Gateway Pools** page appears.

2. Click **New Gateway Pool**.
3. In the **New Gateway Pool** dialog, configure the following details and click **Create**.

Figure 16-2: New Gateway Pool

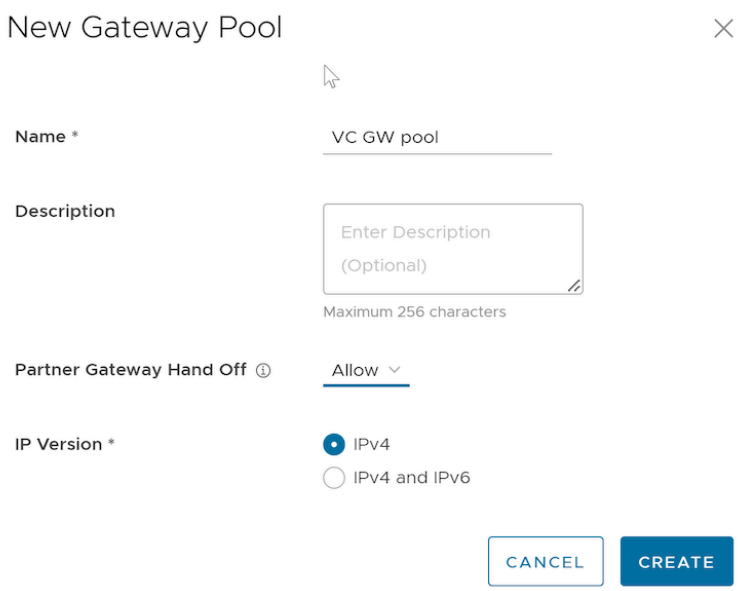


Table 57: New Gateway Pool Field Descriptions

Field	Description
Name	Enter a name for the new Gateway pool.
Description	Enter a description for the Gateway pool.
Partner Gateway Hand Off	This option determines the method for handing off Gateways to Partners. Select one of the following options from the drop-down list: • **None** - Select this option when Partner Gateway handoff is not required. • **Allow** - Select this option when users want the Gateway pool to support both Partner Gateways and Cloud Gateways. • **Only Partner Gateways** - Select this option when Edges in the Enterprise should not be assigned with Cloud Gateways from the pool, and will only be assigned with the Gateways set for an individual Edge.
IP Version	Select one of the following address types with which users want to activate the Gateway pool: • **IPv4** - Allows adding IPv4-only Gateways. • **IPv4 and IPv6** - Allows adding Gateways with IPv4 and IPv6 addresses. **Note:** If users want to use Edges with IPv6 support, then choose **IPv4 and IPv6**.

Configure the Gateway pool by adding Gateways to the pool. See Configure Gateway Pools.

16.1.2 Clone a Gateway Pool

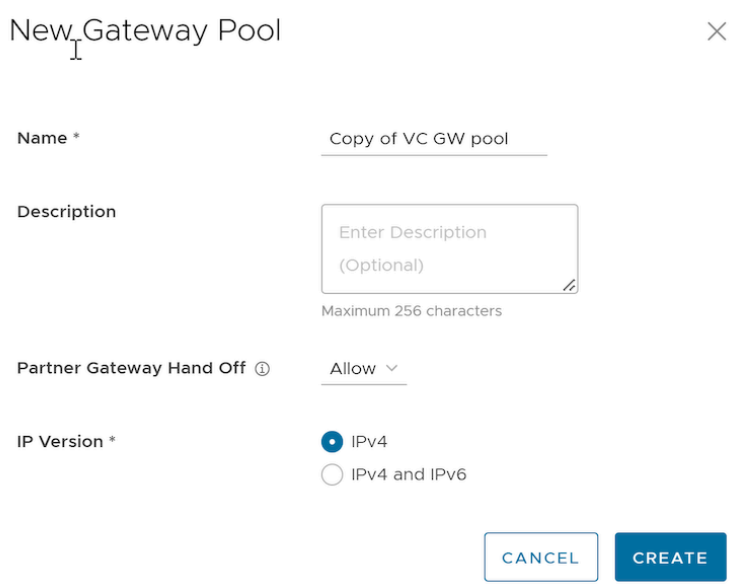
Users can clone the configurations from an existing Gateway pool and create a new Gateway pool with the cloned settings.

1. In the **Orchestrator UI**, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane.

   The **Gateway Pools** page appears.
2. In the **Gateway Pools** table, select the Gateway pool that users want to clone and click **Clone**.

   The **New Gateway Pool** dialog appears with the cloned settings.

   Figure 16-3: Clone a Gateway Pool



   The Gateway pool clones the existing configuration from the selected Gateway pool. If required, modify the details. For additional information on the options, see Create New Gateway Pool.
3. After updating the Gateway pool details, click **Create**.

Configure the Gateway pool by adding Gateways to the pool. See Configure Gateway Pools.

16.1.3 Configure Gateway Pools

After creating a Gateway pool, users can add Gateways to the pool and associate the pool with an Enterprise Customer.

Whenever users create a new Gateway pool or clone a pool, the UI redirects to the **Gateway Pool Overview** page to configure the Gateway pool's properties.

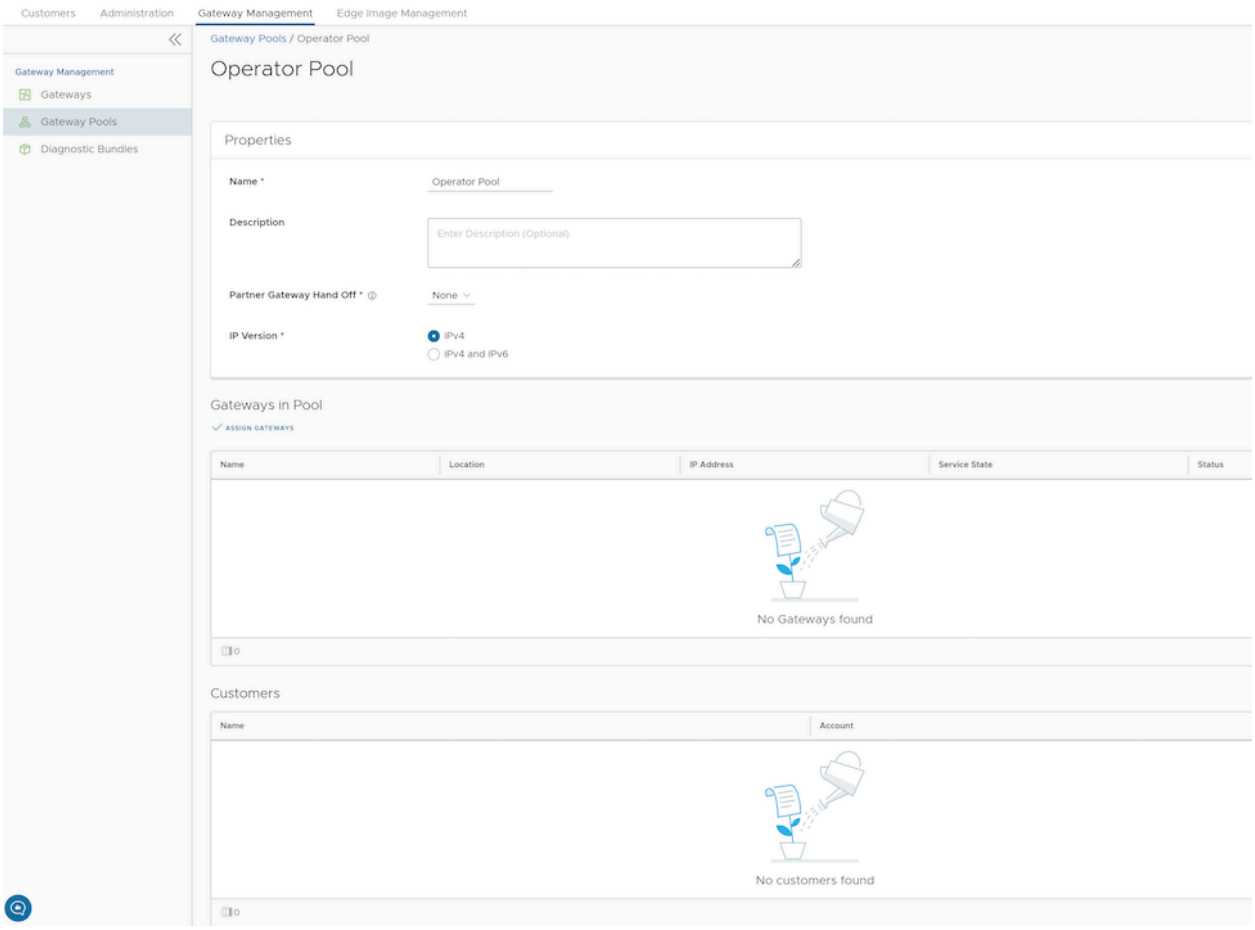
To configure an existing Gateway pool:

1. In the **Orchestrator UI**, select the **Gateway Management** tab and go to **Gateway Pools** in the left navigation pane.

   The **Gateway Pools** page appears.
2. Click the name link for the **Gateway pool** the user wants to configure.

3. Configure the following details for the Gateway pool:

Figure 16-4: Configure Operator Pool



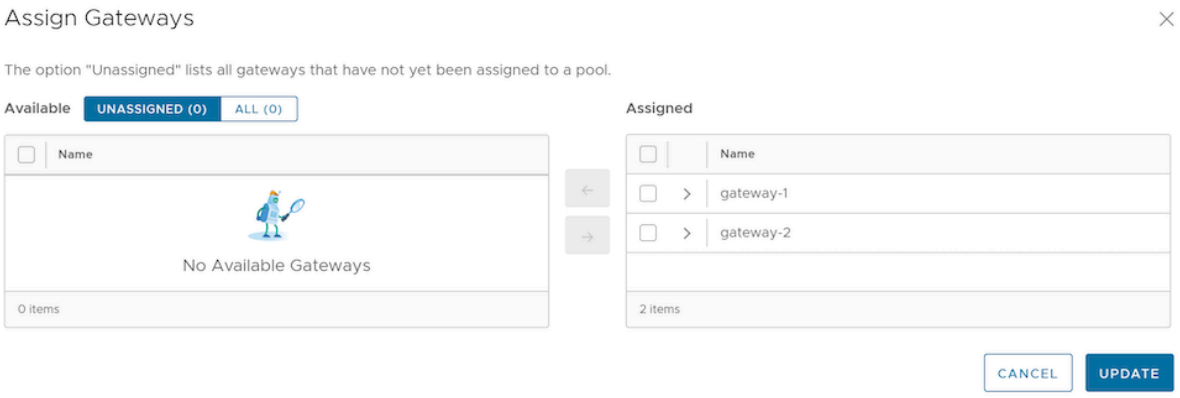
a. In the **Properties** section, the system displays the current Name, Description, Partner Gateway Handoff details, and Association Type. If required, modify these details.

b. In the **Gateways in Pool** section, click **Manage** to add Gateways to the pool.

The **Assign Gateways to Gateway pool** dialog appears.

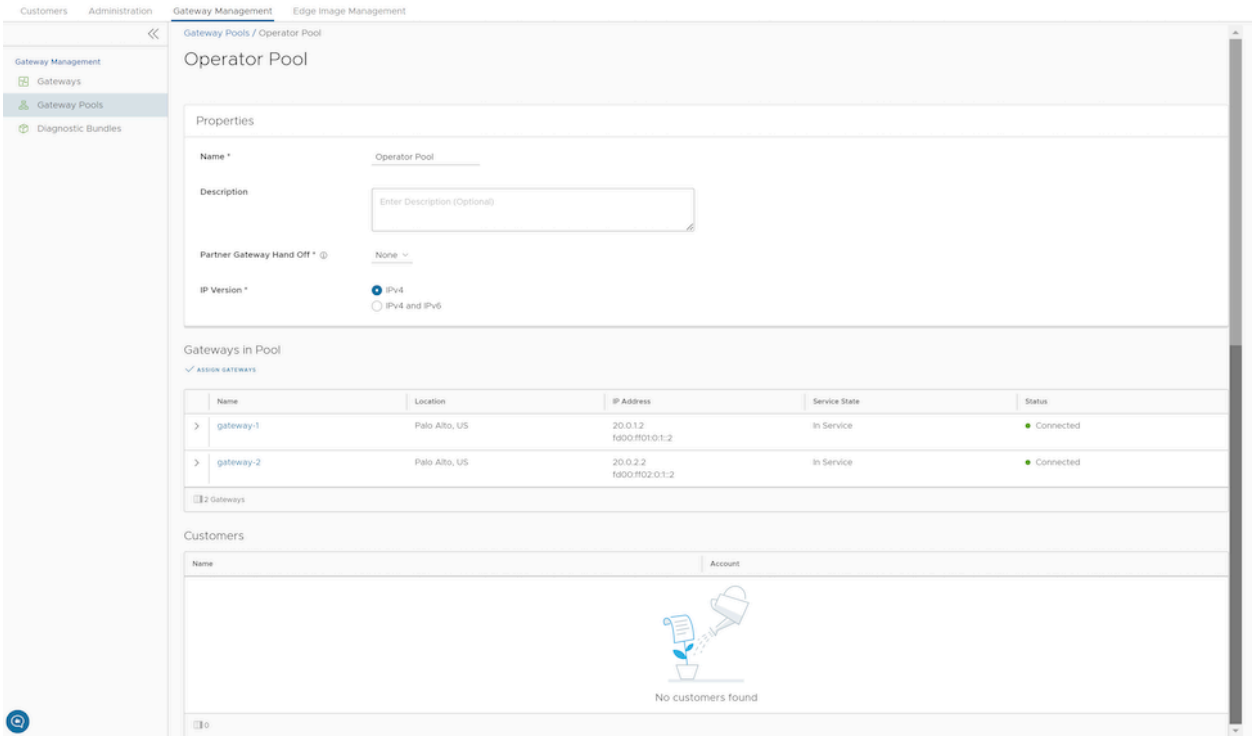
c. In the **Assign Gateways to Gateway pool** dialog, move the required Gateways from the **Available** pane to the **Assigned** pane using the Arrows and click **Update**.

Figure 16-5: Assign Gateways



4. The Gateways assigned to the selected Gateway pool are displayed as follows:

Figure 16-6: Assigned Gateways in Pool



5. Click **Save Changes**.

The configured Gateway pools are displayed in the **Gateway Pools** page.

Users can associate the Gateway Pool with either a Partner or a specific Enterprise Customer. After association, the Edges within that Enterprise connect to the available Gateways in the pool to establish their control plane and data paths.

Refer to the following links to associate the Gateway pool:

- For a new customer, see Create New Customer.
- For an existing customer, see Configure Customers.
- For a new Partner, see Create New Partner.
- For an existing Partner, see Configure Partner.

16.2 Manage Gateways

Arista SD-WAN Gateways are a distributed network of gateways deployed worldwide or on-premises at service providers that provide scalability, redundancy, and on-demand flexibility. The Gateways optimize data paths to all applications, branches, and data centers and enable the delivery of network services to and from the cloud.

By default, the Gateways named *gateway-1* and *gateway-2* are available when users install Orchestrator. If required, users can create additional Gateways.

The Operator Super user and Operator Admin user can create, manage, and delete Gateways created by both Operator and Partner users.

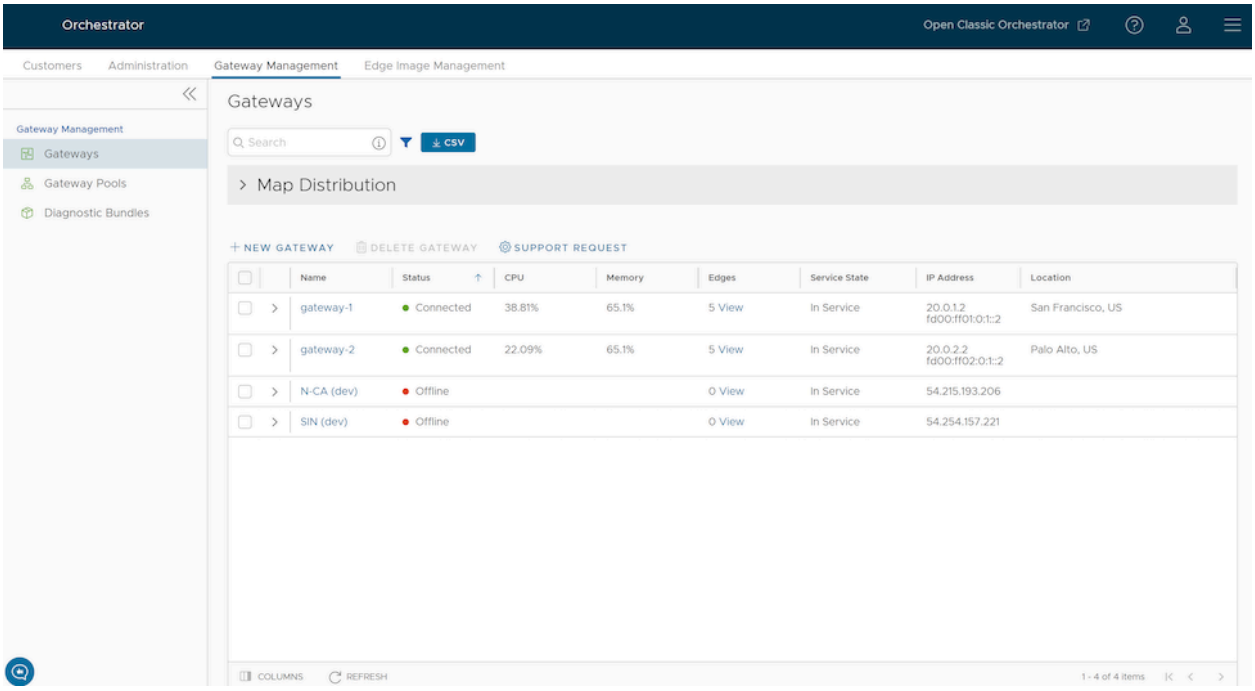
Note: The Operator IT support user and Operator Business Specialist user can only view the configured Gateways.

To manage Gateways, perform the following steps:

1. Log in to the **Orchestrator** as an Operator Super user or Admin user.
2. In the **Orchestrator UI**, select the **Gateway Management** tab and go to **Gateways** in the left navigation pane.

The **Gateways** page appears.

Figure 16-7: Manage Gateways



To search a specific Gateway, enter a relevant search text in the **Search** box. For advanced search, select the **filter** icon next to the **Search** box to filter the results by specific criteria.

The **Map Distribution** section displays the Gateways on a map. Users can click the **+** and **-** buttons to zoom in and zoom out the map, respectively.

The **Gateways** table displays the existing Gateways with the following details:

Table 58: Existing Gateways Field Descriptions

Field	Description
Name	Name of the Gateway
Status	Reflects the success or failure of periodic heartbeats sent by mgd to the Orchestrator and does not indicate the status of the data and control plane. The following are the possible statuses: • **Connected** – Gateway is heart beating successfully to the Orchestrator. • **Degraded** – Orchestrator has not heard from the Gateway for at least one minute. • **Offline** – Orchestrator has not heard from the Gateway for at least two minutes.
CPU	Average CPU utilization of all the cores in the system at the time of the last heartbeat.
Memory	Percentage usage of the physical memory by all processes in the system as reported by `psutil.phymem_usage` at the time of the last heartbeat. This is similar to estimating memory usage with the `free` command.
Edges	Number of Edges connected to the Gateway at the time of the last heartbeat. **Note:** Click **View** next to the number of Edges to view all Edges assigned to the Gateway and their online/offline status in Orchestrator. This option does not display the Edges that are actually connected to the Gateway.
Service State	The user-configured service state of the Gateway and whether it is eligible to be assigned to new Edges.
IP Address	The public IP address that the public WAN links of an Edge use to connect to the Gateway. This IP address uniquely identifies the Gateway. If the Gateway is enabled to accommodate both IPv4 and IPv6 addresses, this column displays both IP addresses.
Location	Location of the Gateway from GeoIP (by default) or as manually entered by the user. This is used for geographic assignment of the Gateway to Edges and should be verified.

On the **Gateways** page, users can perform the following activities:

- **New Gateway** - Creates a new Gateway. See Create New Gateway with New Orchestrator UI.
- **Delete Gateway** - Deletes a selected Gateway only if it is currently idle. The system prevents users from deleting any Gateway that a Partner or an Enterprise Customer is actively using, ensuring that users do not accidentally disrupt live network traffic or disconnect active Edges.
- **Stage to Bastion** - Stages a Gateway to the Bastion Orchestrator.
- **Unstage from Bastion** - Removes a Gateway from the Production Orchestrator.

  Note: Stage to Bastion and **Unstage from Bastion** options are available only when the Bastion Orchestrator feature is enabled using the `session.options.enableBastionOrchestrator` system property.

  For additional information, see *Bastion Orchestrator Configuration Guide*.

- **Support Request** - Redirects to a Knowledge Base article that has instructions on how to file a support request.

16.2.1 Create New Gateway

In addition to the default Gateways, users can create Gateways and associate them with Enterprise Customers.

To create a Gateway, perform the following steps.

1. Select the **Gateway Management** tab and go to **Gateways** in the left navigation pane. The **Gateways** page appears.
2. Select **New Gateway**. The **New Gateway** dialog appears.
3. In the **New Gateway** dialog, configure the following details:

Figure 16-8: Create a New Gateway

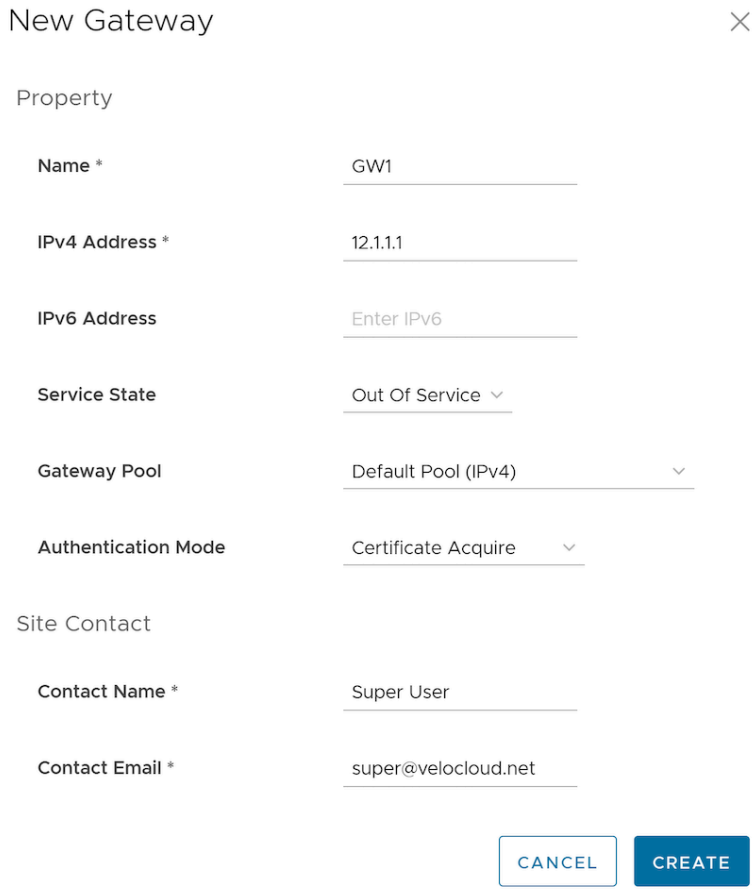


Table 59: New Gateway Field Descriptions

Field	Description
Name	Enter a name for the new Gateway.
IPv4 Address	Enter the IPv4 address of the Gateway.
IPv6 Address	Enter the IPv6 address of the Gateway.
Service State	Select the Gateway's service state from the drop-down list. The following options are available: • **In Service** - The Gateway is connected and available. • **Out of Service** - The Gateway is not connected. • **Quiesced** - The Gateway service is quiesced or paused. Select this state for backup or maintenance purposes. **Note:** The **Quiesced** and **Out of Service** states are only applicable for Cloud Gateway deployment.
Gateway Pool	Select the Gateway Pool from the drop-down list to assign the Gateway to a specific group.
Authentication Mode	Select the authentication mode of the Gateway from the following available options: • **Certificate Not Required** - Gateway uses pre-shared key authentication. • **Certificate Acquire** - This option is selected by default and instructs the Gateway to acquire a certificate from the Orchestrator's certificate authority, by generating a key pair and sending a certificate signing request to the Orchestrator. After acquisition, the Gateway uses the certificate for authentication with the Orchestrator and for establishing VCMP tunnels. **Note:** After acquiring the certificate, the option can be updated to **Certificate Required**. **Note:** When users enable the Bastion Orchestrator feature, users must set the Authentication mode for the staged Gateways to either **Certificate Acquire** or **Certificate Required**. • **Certificate Required** - Gateway uses the PKI certificate. Operators can change the certificate renewal time window for Gateways using the system properties.
Contact Name	Enter the name of the Site Contact.
Contact Email	Enter the Email ID of the Site Contact.

Note:

- After users have created a Gateway, they cannot modify the IP addresses.
- Release 4.3.x and 4.4.x supports Greenfield deployment of Gateways for IPv6. If users have upgraded a Gateway from a previous version earlier than 4.3.0, they cannot configure the upgraded Gateway with the IPv6 address.
- Release 4.5.0 supports both the Greenfield and Brownfield deployment of Gateways for IPv6. If users have upgraded a Gateway from a previous version earlier than 4.5.0, they can dynamically configure an IPv6 address for the Gateway.
- The system does not support IPv4/IPv6 dual-stack mode for Bastion Orchestrator configurations.

After users create a new Gateway, the system redirects them to the Configure Gateways page. From here, users can configure additional settings, such as BGP handoff details, location parameters, and pool assignments, to fully integrate the Gateway into your network

To configure additional Gateway settings, see Configure Gateways.

16.2.2 Configure Gateways

When users create a new Gateway, the Orchestrator UI automatically redirects them to the **Configure Gateways** page, where they can configure Gateway properties and additional settings.

To configure an existing Gateway, perform the following steps

1. In the **Operator** portal of the Orchestrator, select the **Gateway Management** tab and go to **Gateways** in the left navigation pane. The **Gateways** page displays the list of available Gateways.
2. Click the Gateway link to configure additional settings. The system displays the details of the selected Gateway in the **Configure** > **Gateways** page.
3. On the **Overview** tab, configure the following details:

Figure 16-9: Configure Gateways

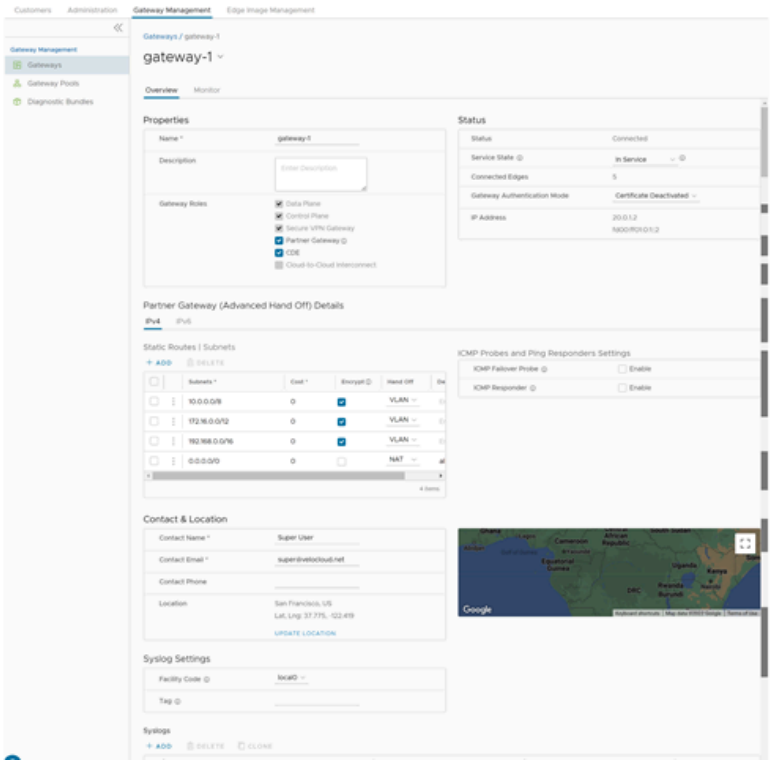


Table 60: Gateway Option Descriptions

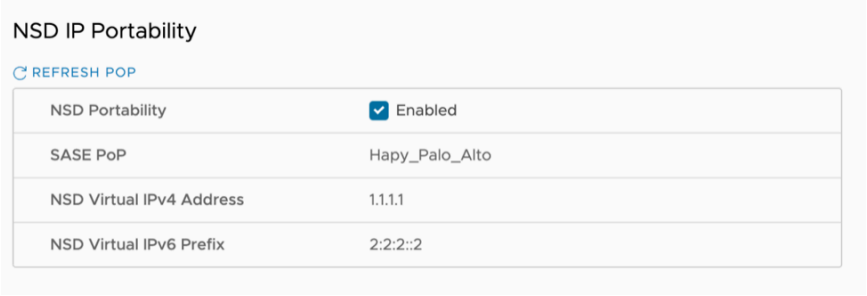
Option	Description

Status	Users can configure the following details:
	• **Status:** Displays the status of the Gateway, which reflects the success or failure of periodic heartbeats sent to the Orchestrator. The following are the available statuses:
	  • **Connected:** Gateway is heart beating successfully to the Orchestrator.
	  • **Degraded:** Orchestrator has not heard from the Gateway for at least one minute.
	  • **Offline:** Orchestrator has not heard from the Gateway for at least two minutes.
	• **Service State:** Select the Service State of the Gateway from the following available options:
	  • **In Service:** The Gateway is connected and available for Primary or secondary tunnel assignments. When the Service state of the Gateway is switched from 'Out Of Service' to 'In Service', the Primary or Secondary assignments, Super Gateways, and Edge-to-Edge routes are recalculated for each Enterprise using the Gateway.
	  • **Pending Service:** The Gateway is connected and awaiting tunnel assignments.
	  • **Out of Service:** The Gateway is not connected or not available for any assignments. The system removes all existing assignments.
	  • **Quiesced:** When users quiesce or pause the Gateway service, the system prevents the addition of any new tunnels or Non-SD-WAN (NSD) sites. However, the existing assignments would remain in the Gateway. Select this state for backup or maintenance purposes.
	  Note: The **Quiesced** and **Out of Service** states are only applicable for Cloud Gateway deployment.
	  When users quiesce the Gateway service, Orchestrator provides self-service migration functionality that allows users to migrate from an existing Gateway to a new Gateway without Operator support.
	  For additional information, see Quiesce Gateways.
	  Note: VeloCloud SD-WAN does not support Self-service migration on Partner Gateways.

Connected Edges	Displays the number of Edges connected to the Gateway. This option is displayed only when the Gateway is activated.

Option	Description

Gateway Authentication Mode	Select the authentication mode of the Gateway from the drop-down menu:
	• **Certificate Deactivated:** Gateway uses a pre-shared key for authentication. If users change the mode from **Certificate Deactivated** to:
	  • **Certificate Acquire:** Tunnels in PSK mode are not affected. Only tunnels with Gateways get impacted. These tunnels are reconnected based on the certificate. All tunnels configured in PSK mode remain active, and no traffic disruptions are observed.
	  • **Certificate Required:** The Orchestrator prevents users from making this change directly. Users must first change the mode to **Certificate Acquire**, and then change it to **Certificate Required**. This helps avoid heartbeat loss to the Orchestrator when Edge is assigned a certificate.
	• **Certificate Acquire:** The system selects this option by default and instructs the Gateway to acquire a certificate from the Orchestrator's certificate authority, by generating a key pair and sending a certificate signing request to the Orchestrator. After acquisition, the Gateway uses the certificate for authentication with the Orchestrator and for establishing VCMP tunnels. If users change the mode from **Certificate Acquire** to:
	  • **Certificate Deactivated:** PSK-based tunnels are not impacted. Tunnels with Gateways and all certificate-based tunnels are disconnected and reconnected based on PSK.
	  • **Certificate Required:** All peers configured with PSK mode are disconnected and cannot connect to the Hub. All current RSA tunnels stay active.
	While the Hub is in **Certificate Acquire** mode, the system reestablishes all certificate-based tunnels using a new certificate. This process ensures a seamless transition to updated credentials without manual intervention. Importantly, the system maintains all PSK-based tunnels without interruption, as these connections do not rely on the certificate exchange process.
	Note: After acquiring the certificate, users can update the option to **Certificate Required**.
	• **Certificate Required:** Gateway uses the PKI certificate. Operators can change the certificate renewal time window for Gateways using the system property `gateway.certificate.renewal.window`. If users change the mode from Certificate Required to:
	  • **Certificate Deactivated:** All peers with an RSA tunnel are disconnected and cannot reconnect. All peers configured in PSK mode remain active, and no disruption is observed in traffic.
	  • **Certificate Acquire:** All peers configured in PSK mode reconnect with the Hub/Gateway. All current RSA tunnels stay active.
	Note:
	• When the Gateway certificate is revoked, the Gateway does not receive the certificate revocation list (CRL), as it loses the Transport Layer Security (TLS) connection immediately. Anyway, the Gateway is still operable.
	• The current QuickSec design checks the validity of CRL time. The CRL's time validity must match the current time at Edges for the CRL to affect a newly established connection. To implement this, ensure the Orchestrator time is properly updated to match the Edges' date and time.

Option	Description
IP Address	Displays the public IP address that the public WAN links of an Edge use to connect to the Gateway. This IP address uniquely identifies the Gateway. If users have configured the Gateway with both IPv4 and IPv6 addresses, this field displays both IP addresses. If users have created an IPv4-only Gateway or if there is an existing IPv4 Gateway upgraded from previous versions, users can enter the IPv6 address to support the dual stack. After saving the changes, the IPv6 address is not sent to the Edges immediately. Users can trigger the rebalance operation to push the IPv6 address to the customer and the associated Edges manually, or the IPv6 address is sent to the Edges during the next Control Plane update. **Note:** Adding an IPv6 address is a one-time activity. After users save the changes, they cannot modify the IP addresses. **CAUTION:** An incorrectly configured IPv6 address when pushed to Edges might cause IPv6 tunnelling to the IPv6 Gateway to fail. In such cases, users need to deactivate the Gateway and create a new one to activate both the IPv4 and IPv6 addresses.
Contact & Location	Displays the existing contact details. If required, users can modify the information.
NSD IP Portability	Beginning with the 6.0 Orchestrator release, selecting this option will activate NSD IP Portability for the Gateway. Portable NSD IPs allow Operators to move NSD configurations to different Gateways in the POP without requiring the customer to reconfigure their tunnels. When the **NSD Portability** checkbox is selected, the Orchestrator fetches the following data, such as Point of Presence (PoP) name, NSD Virtual IPv4 Address, and NSD Virtual IPv6 Prefix currently assigned to the Gateway from the Global Services Manager (GSM) and displays it. Click **Refresh POP** to retrieve the current and updated data. **Note:** For the "NSD Portability" feature to work as designed, the Operators must ensure that the Gateways are associated with the corresponding PoPs in GSM. **Figure 16-10: NSD IP Portability**  **Important:** There are two important caveats with NSD IP Portability: **a.** NSD peers must operate as an IKE responder. In the past, some configurations would permit an initiator-only set up, but that will no longer function. **b.** Peers must allow Network Address Translation Traversal (NAT-T). The current implementation of NSD Portable IP uses NAT, which is implemented internally within the POP.
Syslog Settings	Beginning with the 4.5 release, Gateways can export NAT information via a remote syslog server or via Telegraph to the desired destination. For additional information, see the *Configure NAT Entry Syslog for Gateways* section in the *VeloCloud SD-WAN Operator Guide*.
Customer Usage	Displays usage details for different types of Gateways assigned to customers.
Pool Membership	Displays the details of the Gateway Pools to which users have assigned the current Gateway.
Partner Gateway (Advanced Handoff) Details	This section is available only if users select the **Partner Gateway** checkbox. Users can configure advanced handoff settings for the Partner Gateway. For additional information, see the *Partner Gateway (Advanced Handoff) Details* section later.

Partner Gateway (Advanced Handoff) Details - Users can configure the following advanced handoff settings for the Partner Gateway:

CAUTION: VeloCloud does not recommend pushing IPv6 configurations to Partner Gateways running software versions earlier than 5.0.

Table 61: Partner Gateway Option Descriptions

Option	Description
Static Routes | Subnets - Specify the subnets or routes that the Gateway should advertise to the Edge. This is global per Gateway and applies to all customers. With BGP, this section is used only if there is a shared subnet that all customers need to access and if NAT handoff is required. Remove the unused subnets from the Static Route list if users do not have any subnets to advertise to the Edge and have the handoff of type NAT. Users can select the **IPv4** or the **IPv6** tab to configure the corresponding address type for the Subnets.	
Subnets	Enter the IPv4 or IPv6 address of the Static Route Subnet that the Gateway should advertise to the Edge.
Cost	Enter the cost to apply weighting on the routes. The range is from 0 to 255.
Encrypt	Select the checkbox to encrypt the traffic between Edge and Gateway.
Hand off	Select the handoff type as VLAN or NAT.
Description	Optionally, enter a descriptive text for the static route.
ICMP Probes and Ping Responders Settings **ICMP Failover Probe** - The Gateway uses an an ICMP probe to check the reachability of a particular IP address. It notifies the Edge to failover to the secondary Gateway if the IP address is unreachable. This option supports only IPv4 addresses.	
VLAN Tagging	Select the VLAN tag from the drop-down list to apply to the ICMP probe packets. The following are the available options: • **None:** Untagged • **802.1q:** Single VLAN tag • **802.1ad:** / **QinQ(0x8100)** / **QinQ(0x9100):** Dual VLAN tag
Destination IP address	Enter the IP address to be pinged.
Frequency	Enter the time interval, in seconds, to send the ping request. The range is from 1 to 60 seconds.
Threshold	Enter the number of times the system can miss ping replies before it marks the routes as unreachable. The range is from 1 to 10.
ICMP Responder - Allows the Gateway to respond to ICMP probes from the next-hop router when the tunnels are up. This option supports only IPv4 addresses.	
IP address	Enter the virtual IP address that will respond to the ping requests.
Mode	Select one of the following modes from the drop-down list: • **Conditional** - Gateway responds to ICMP requests only when the service is up and at least one tunnel is up. • **Always** - Gateway always responds to the ICMP request from the peer.

Note: The ICMP probe parameters are optional and recommended only if users want to use ICMP to check the Gateway's health. With BGP support on the Partner Gateway, using an ICMP probe for failover and route convergence is no longer required. For additional information on

configuring BGP support and handoff settings for a Partner Gateway, see Configure a Handoff Operator.

4. After configuring the required details, click **Save Changes**.

16.2.3 Upgrade Orchestrator for Dual Stack Support

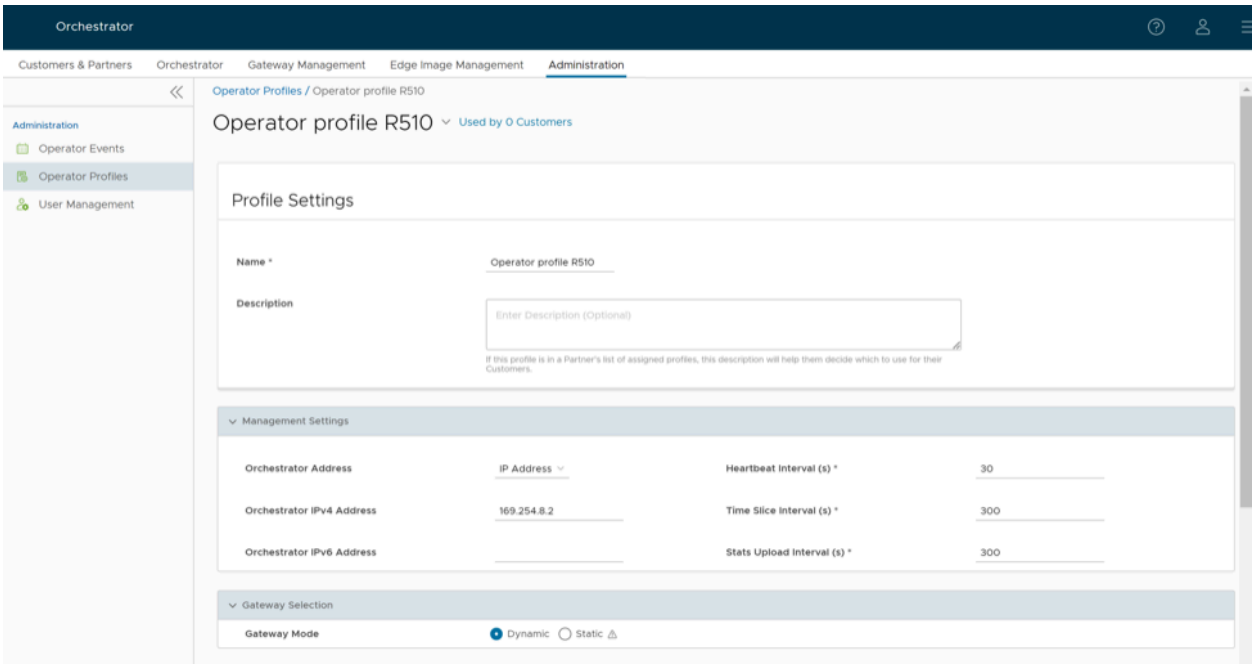
To upgrade Orchestrator to release 5.0.0 to support dual stack, perform the following:

- Upgrade Orchestrator to release 5.0.0.
- Add an IPv6 address in the Orchestrator Shell. The following example shows a sample configuration:

```
vcadmin@vco:~$ cat /etc/netplan/50-cloud-init.yaml
network:
 ethernets:
  eth0:
   addresses: [169.254.8.2/29, 'fd00:aaaa:0:1::2/64']
   routes:
   - {metric: 1, to: 0.0.0.0/0, via: 169.254.8.1}
   - {metric: 1, to: '0::0/0', via: 'fd00:aaaa:0:1::1'}
 renderer: networkd
 version: 2
```

- In the Orchestrator's Operator portal, navigate to **Administration** > **Operator Profiles**, and select a Profile.
- On the **Operator Profiles** page of the selected Profile, navigate to the **Management Settings** section and enter the IPv6 address configured in Orchestrator Shell.

Figure 16-11: Configure Operator Profile



- Click **Save Changes**.

16.2.4 Configure IPv6 Address on Gateways

Enterprise users can provision a Gateway with both IPv4 and IPv6 addresses.

Prerequisites

Ensure that the Orchestrator is running version 5.0.0 as described in Upgrade Orchestrator for Dual Stack Support.

Deploy VeloCloud Gateway on AWS

Consider the following guidelines while deploying Gateways on AWS.

- While migrating Gateways to the cloud, it is recommended to destroy and create a new instance with IPv6 enabled.
- When a VeloCloud Gateway is freshly deployed in the AWS portal with IPv6 selected, it is required to use only static IPv4/IPv6 address assignment on the Gateway's interfaces, as VeloCloud SD-WAN does not support DHCP on the Gateway side.

Set up IPv6 Address on Gateways for a New Deployment

1. Create a Gateway pool with **IPv4 and IPv6** IP version types.
2. Deploy a new Gateway with version 5.0.0. User can configure IPv4 and IPv6 addresses on the public interface using netplan if IPv6 is not available in meta-data.

   The following example shows a sample configuration:

```
vcadmin@vcg2:~$ cat /etc/netplan/50-cloud-init.yaml
network:
 ethernets:
  eth0:
   addresses: [169.254.10.2/29, 'fd00:ff01:0:1::2/64']
   routes:
   - {metric: 1, to: 0.0.0.0/0, via: 169.254.10.1}
   - {metric: 1, to: '0::0/0', via: 'fd00:ff01:0:1::1'}
  eth1:
   addresses: [101.101.101.11/24]
   routes:
   - {metric: 2, to: 0.0.0.0/0, via: 101.101.101.10}
  eth2:
   addresses: [192.168.0.111/24]
 renderer: networkd
 version: 2
vcadmin@vcg2:~$
```

3. After updating the netplan, run sudo netplan apply to apply the configuration.

```
vcadmin@vcg2:~$ sudo netplan apply
vcadmin@vcg2:~$
```

4. Activate the Gateway using the Orchestrator's IPv4 address. If the Orchestrator is provisioned with dual stack, Te user can activate the Gateway using either the IPv4 or IPv6 address of the Orchestrator.
5. After activation, the Orchestrator will push both IPv4 and IPv6 information to the Edges.
6. Upgrade Edge's software version to 5.0.0. After the Edges are upgraded, the Orchestrator enables options to set up IPv6-related device settings.

Set up IPv6 Address on Gateways Upgraded from Previous Release

1. Upgrade the Gateways to release 5.0.0.
2. In the Gateway shell, update the netplan configuration to include an IPv6 address. The following example shows a sample configuration:

```
vcadmin@vcg2:~$ cat /etc/netplan/50-cloud-init.yaml
network:
```

```
 ethernets:
  eth0:
   addresses: [169.254.10.2/29, 'fd00:ff01:0:1::2/64']
   routes:
   - {metric: 1, to: 0.0.0.0/0, via: 169.254.10.1}
   - {metric: 1, to: '0::0/0', via: 'fd00:ff01:0:1::1'}
  eth1:
   addresses: [101.101.101.11/24]
   routes:
   - {metric: 2, to: 0.0.0.0/0, via: 101.101.101.10}
  eth2:
   addresses: [192.168.0.111/24]
 renderer: networkd
 version: 2
vcadmin@vcg2:~$
vcadmin@vcg2:~$ sudo netplan apply
vcadmin@vcg2:~$
```

3. In the Orchestrator portal, navigate to the **Gateways** page and select the upgraded IPv4 Gateway.
4. On the **Overview** page of the selected Gateway, under the **Status** section, enter the IPv6 address configured in the Gateway Shell.

   For additional information, see Configure Gateways.
5. The Orchestrator will push the IPv6 configurations to the Edges.
6. Upgrade Edge's software version to 5.0.0. After the Edges are upgraded, the Orchestrator enables options to set up IPv6-related device settings.
7. Users must rebalance Gateways at the Edge level or for the entire Enterprise Customer for the Edges to receive the Gateway's IPv6 information from Orchestrator.

For additional information, refer to the following topics:

- Manage Gateway Pools
- Manage Gateways
- Manage Operator Profiles

16.2.5 Partner Gateways

Users can configure a Partner Gateway with multiple subnets, and for each subnet, users can assign a specific handoff type: **Network Address Translation (NAT)** or **Virtual Local Area Network (VLAN)**. Additionally, users can define a relative **cost** for each path and specify whether the system should encrypt traffic, giving users granular control over how data exits the SD-WAN overlay and enters your private network.

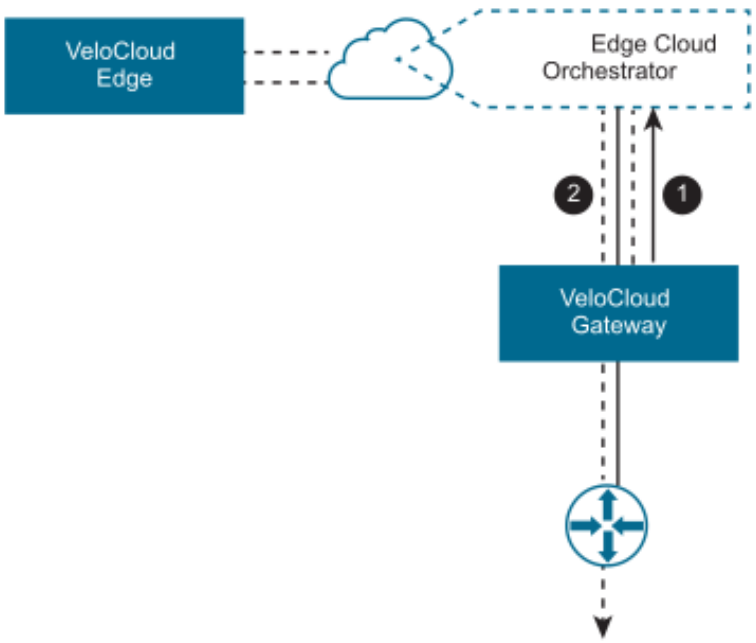
The following examples illustrate two use cases for Partner Gateways configuration.

Gateway Configuration Use Case #1

In the following illustration, the Gateway connects via VLAN/VRF mode to a Virtual Route Forwarding (VRF) instance that lacks public Internet access. However, the Partner Gateway must be able to contact the Orchestrator in the public cloud, and there must be a path to reach the cloud. The Gateway can selectively

NAT certain traffic (such as the IP address of an Orchestrator, or the subnets used to reach public DNS servers) even though it is operating in VLAN/VRF mode.

Figure 16-12: Configure Gateway: Use Case 1



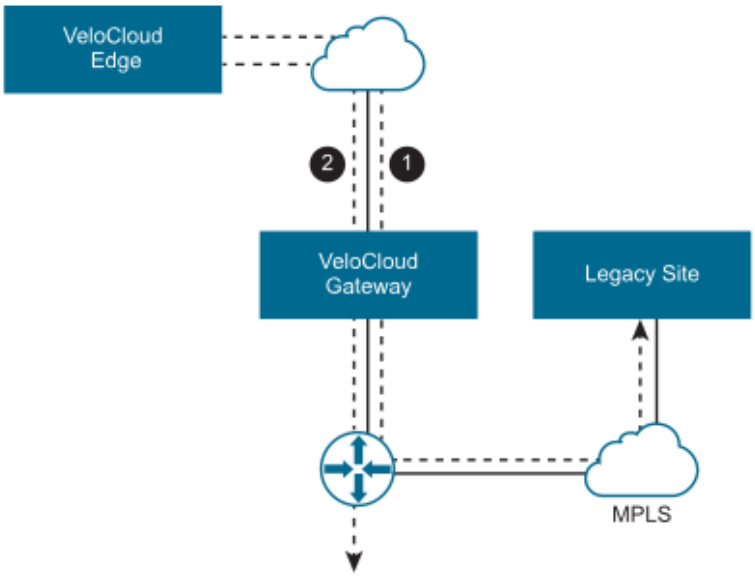
- **#1**- The system routes Orchestrator traffic using IP addresses to NAT.
- **#2**- The system routes Corporate traffic through subnets to VLAN/VRF.

Gateway Configuration Use Case #2

It is common for a Partner Gateway to tie into a corporate network, providing connectivity to legacy sites. This need can occur even when not all corporate sites have been converted to the Arista network. For this use case, it is necessary to specify traffic by subnet on the Partner Gateway. Users can configure each subnet to encrypt network traffic to ensure data remains secure as it passes through the Partner Gateway handoff.

The following illustration shows an example in which only traffic to legacy sites is encrypted. If the Gateway is already configured with a `0.0.0.0/0` subnet to allow all traffic (which is a common configuration), all that would be required is to add the private subnet for your legacy sites and mark it as encrypted.

Figure 16-13: Configure Gateway: Use Case 2



- **#1**- Subnet (e.g., `10.0.0.0/8`) defined for Legacy Sites and marked for encryption. The system transmits traffic between the Edge and the Gateway over an Internet Protocol Security (IPsec) tunnel.
- **#2**- The system sends the remaining traffic unencrypted to the Edge, and then to its final destination.

Note:

- For an IPsec tunnel via the Partner Gateway, a VCMP tunnel failure causes existing flows to time out. The expected behavior for existing flows is to remain on the current path. Any new flow will begin to go (directly), keeping the tunnel down.
- Select application map flags `mustUseGateway` and `dropIfPartnerGatewayDown` to force or drop traffic through the Gateway until the path restores. If these flags are not active, a flow flush is required after the tunnel path restores.

For more information, see the following topics:

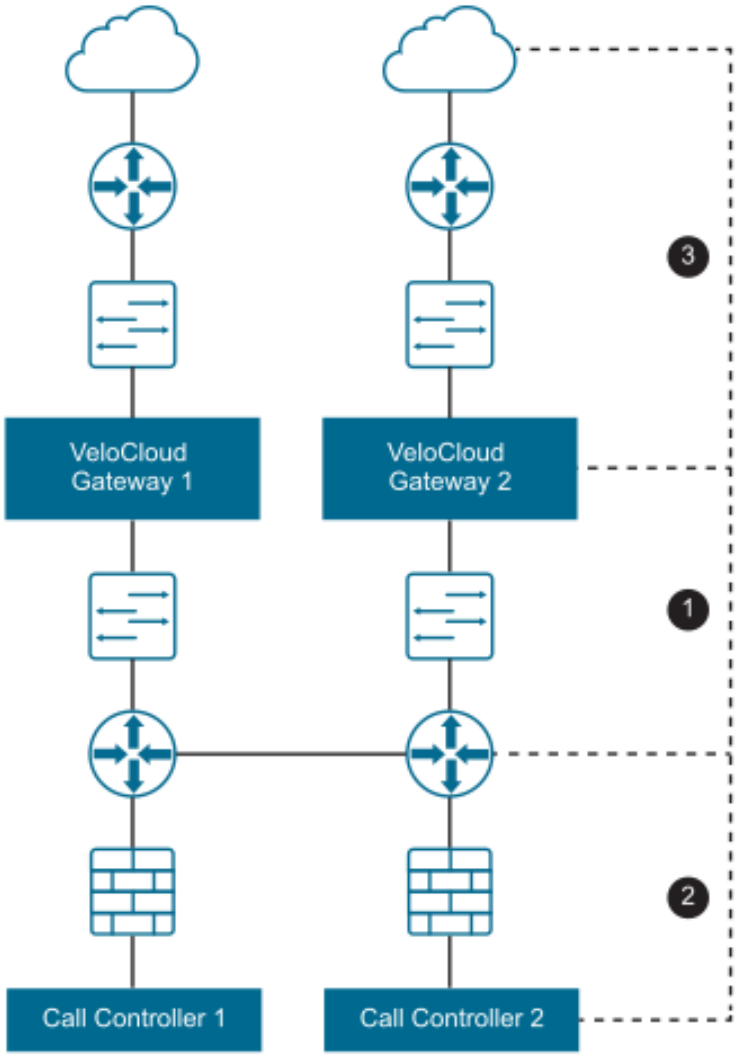
- Partner Gateway Resiliency
- ICMP Failover Probes
- Active/Backup Subnets

16.2.5.1 Partner Gateway Resiliency

The Partner Gateway provides resiliency by detecting failures and failing over to an alternate Partner Gateway. This includes the ability of a Partner Gateway to detect failure conditions and for the surrounding infrastructure to detect failures of the Gateway itself.

Consider the following Gateway topology:

Figure 16-14: Partner Gateway Topology



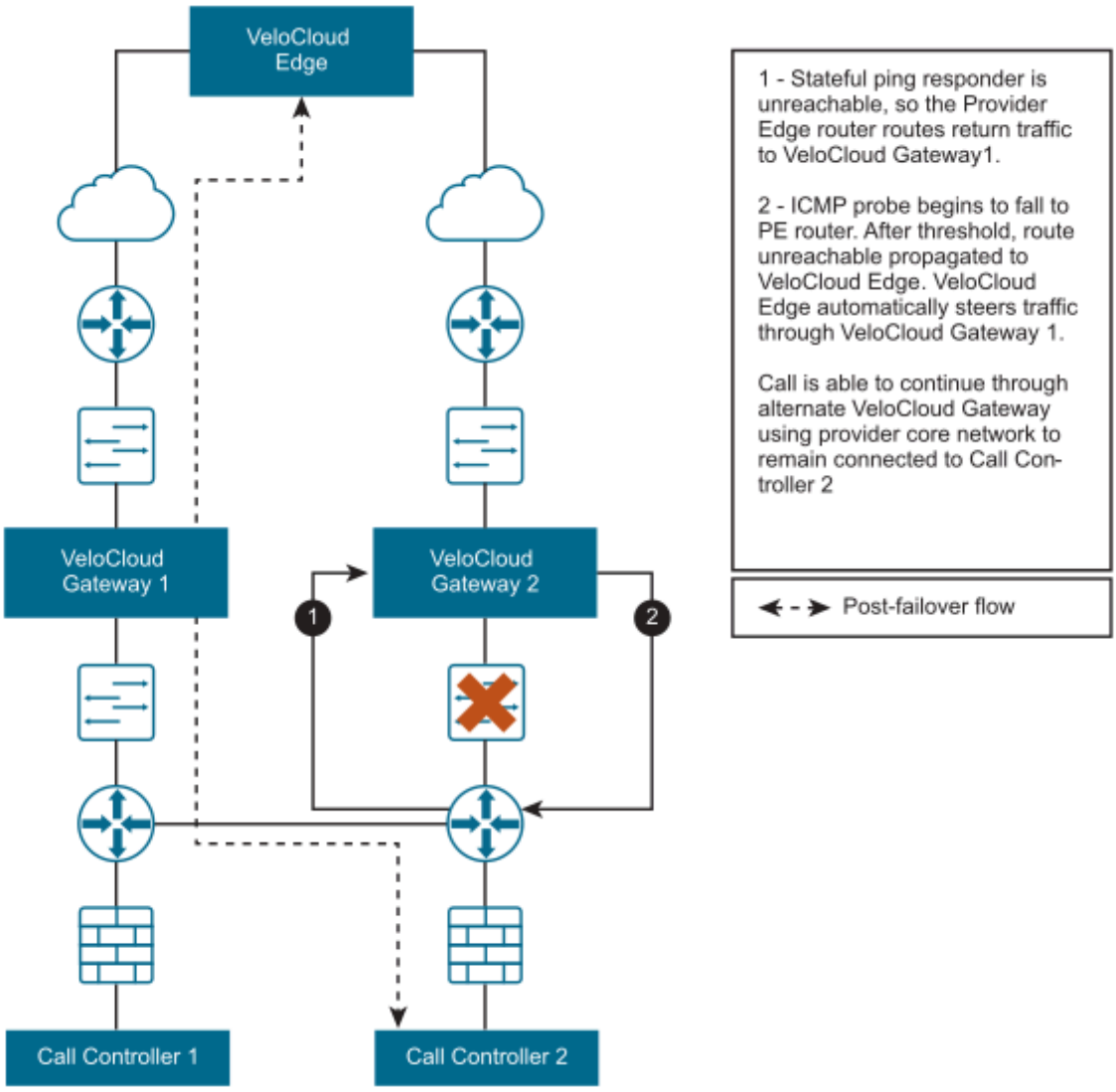
This figure shows three distinct failure zones:

Table 62: Failure Zones

Failure Zone	Component	Description
1	Provider Edge	The Provider Edge is one instance in which failure can be detected either from the Provider Edge router pinging the Gateway, or from the Gateway to the Provider Edge router.
2	Call Controller	The Gateway should be able to ping the Provider Edge router or Call Controller to verify connectivity.
3	WAN	The Gateway should have a stateful ping responder that responds only if the Wide Area Network (WAN) zone is available.

The following figure shows a typical failure scenario that occurs between the Gateway and Provider Edge router and describes the activity that occurs.

Figure 16-15: Failure Scenario Between Gateway and Router



The Partner Gateway also supports configurable route costs, enabling more flexible failure scenarios. Finally, users can assign a handoff type that applies neither Network Address Translation (NAT) nor Virtual Local Area Network (VLAN) tags to the packets. In this configuration, the Gateway passes the packets directly to the Provider Edge router.

16.2.5.2 ICMP Failover Probes

This section discusses ICMP failover probes.

To address a failure in zones #1 or #2 of the Gateway topology diagram, the Gateway supports the optional ability to send failover probes. These probes will ping a single destination IP address at the specified frequency. If the threshold for successive missed ping replies is exceeded, the VeloCloud Gateway will mark the Gateway's routes as unreachable. Even after the system marks the routes as unreachable due to a probe failure, the Edge continues to send probes to the target. This constant monitoring ensures that as soon as the link or service recovers, the system automatically detects the restored connectivity and reactivates the routes.

If the same threshold is exceeded for successive successful ping replies, the Gateway will mark the routes as reachable again.

Example Scenario

For example, consider a user who has configured a frequency of 2 seconds and a threshold of 3.

1. VeloCloud Edges connect to the primary Gateway. The primary Gateway marks routes as reachable.
2. The Primary Gateway fails to receive a reply for three successive probes (~6 seconds).
3. The Primary Gateway marks routes as unreachable and notifies all connected Edges.
4. Edges begin routing Gateway traffic via the alternate Gateway.
5. Connectivity is restored, and the primary Gateway receives three successive probe replies.
6. The Primary Gateway marks routes as reachable and communicates this to all connected Edges.
7. Edges route traffic back through the primary Gateway.

In failure scenario #1, users can configure the system to ping an IP address directly on the Provider Edge (PE) router. This allows users to monitor the health of the immediate physical link or the next-hop availability. In failure scenario #2, users can direct the ping toward the actual Call Controller, enabling the Edge to verify end-to-end reachability for critical voice services.

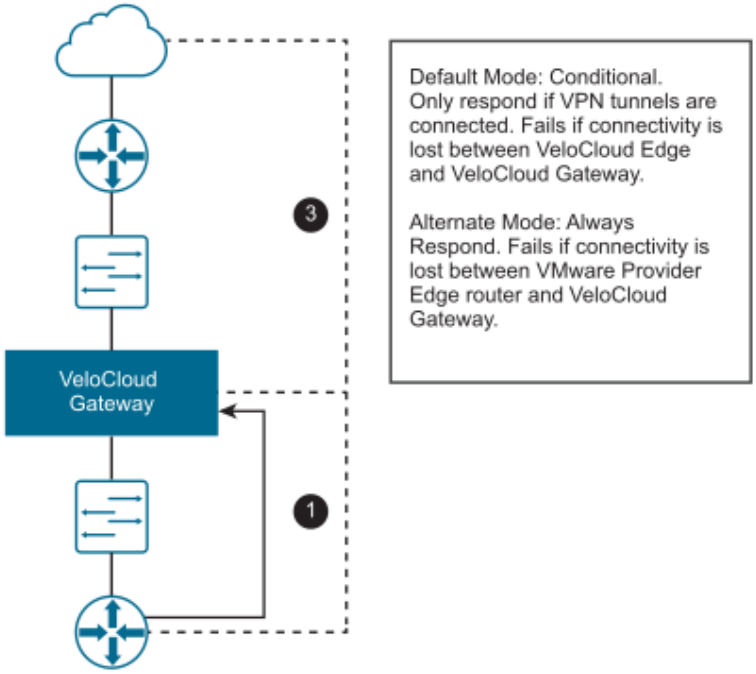
Stateful Ping Responder

To address failures in zones #2 or #3 of the Partner Gateway topology diagram, the Gateway supports an optional stateful ping responder. This allows the configuration of a virtual IP address (which must be different from the interface IP address) within the Gateway that will, based on configuration, either respond to pings always (Gateway service is running) or conditionally based on Wide Area Network (WAN) connectivity (the Gateway has Virtual Private Network (VPN) tunnels connected).

This can be used in failure scenario #1 by having the Provider Edge router ping the ping responder, as the Gateway becoming unreachable would cause the IP SLA on the Provider Edge router to fail. This could also

be used in failure scenario #3 by having the Gateway only respond if VPN tunnels are connected- this is similar to the behavior with BGP (no clients connected means no client routes).

Figure 16-16: Provider Edge Router Ping Responder Scenario



The Partner Gateway will respond to the Provider Edge (PE) router's ICMP request based on the IP SLA configured in the PE router. Users should configure the Stateful Ping Responder PE router as follows, with proper VLAN tag information.

```
!IP-SLA configuration to send ICMP request to gateway virtual IP
ip sla 1
icmp-echo 192.168.10.10 source-ip 192.168.10.1
vrf CUSTOMER1
threshold 1000
timeout 1000
frequency 2
ip sla schedule 1 life forever start-time now

!tracking the IP SLA for its reachability
track 1 ip sla 1 reachability

!all the routes will reachable only when SLA probe succeeds
ip route vrf CUSTOMER1 0.0.0.0 0.0.0.0 192.168.11.101 track 1
ip route vrf CUSTOMER2 0.0.0.0 0.0.0.0 192.168.12.101 track 1
ip route vrf CUSTOMER1 10.0.0.0 255.0.0.0 192.168.10.10 track 1
ip route vrf CUSTOMER2 10.0.0.0 255.0.0.0 192.168.10.10 track 1
ip route vrf CUSTOMER1 192.168.100.0 255.255.255.0 192.168.10.10 track 1
```

Caveats When Using NAT Hand-off Mode

When using Network Address Translation (NAT) hand-off mode, consider the following caveats:

- In VLAN hand-off mode, the Partner Gateway can listen on any IP address if it is reachable from the PE router (including its interface IP). For NAT hand-off mode, the Partner Gateway will not respond if the ICMP request comes to its own interface (WAN) IP address.
- VeloCloud does not support reverse flow in the NAT hand-off mode.

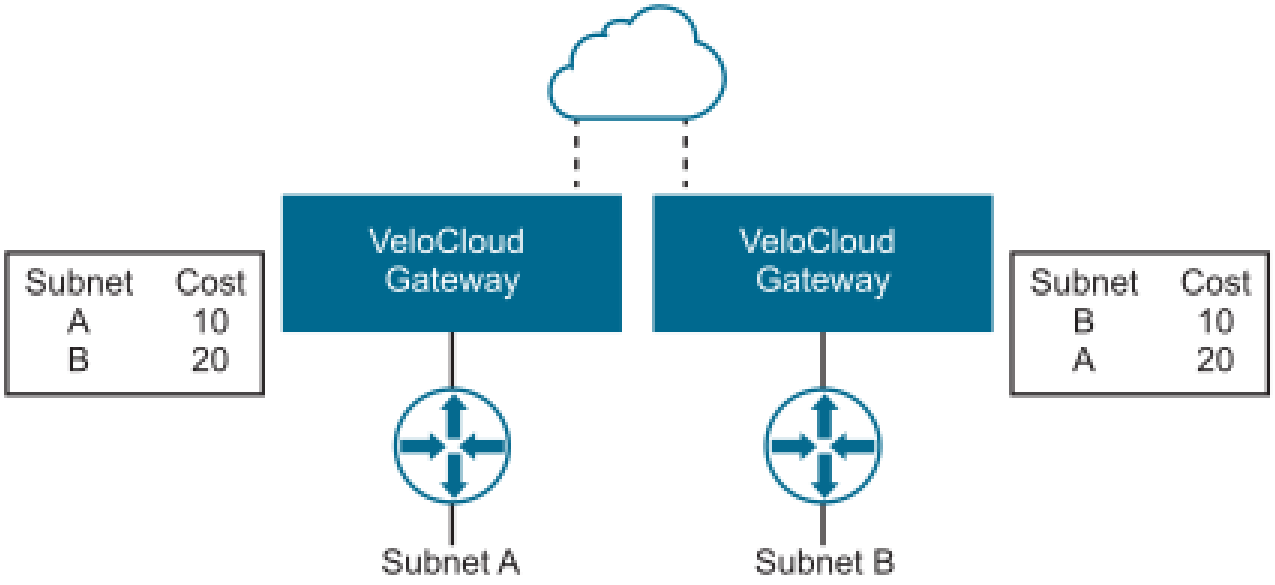
16.2.5.3 Active/Backup Subnets

This section discusses how to configure active and backup subnets for a Partner Gateway.

Subnets on a Partner Gateway

When configuring subnets on a Partner Gateway, users input each subnet along with an optional description to identify the traffic path. By assigning a value to the Cost field, users control route weighting; the system prioritizes lower-cost routes over higher-cost routes to determine the most efficient path for your data. The following figure shows Cost settings per subnet.

Figure 16-17: Partner Gateway Subnets Cost Settings



16.2.6 Monitor Gateways

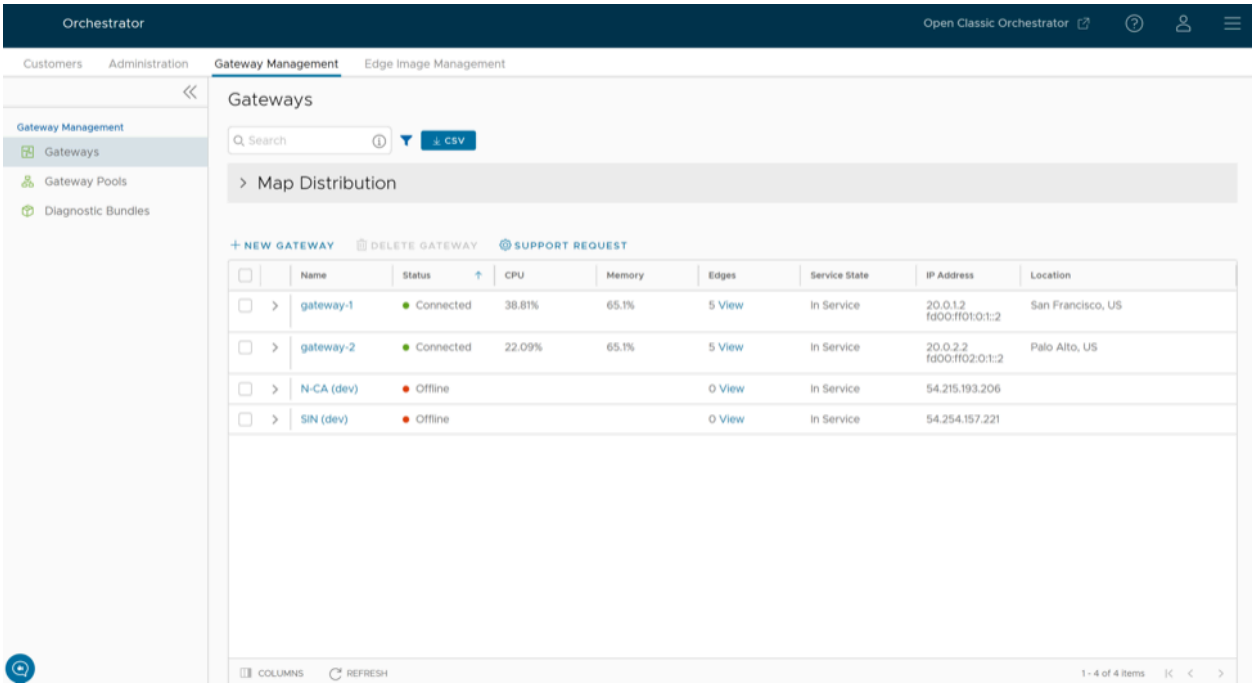
Users can monitor the status and network usage of Gateways in the Operator portal.

To monitor the Gateways:

1. In the **Operator** portal, go to **Gateway Management** > **Gateways**.

2. The **Gateways** page displays the list of available Gateways.

Figure 16-18: Monitor Gateways



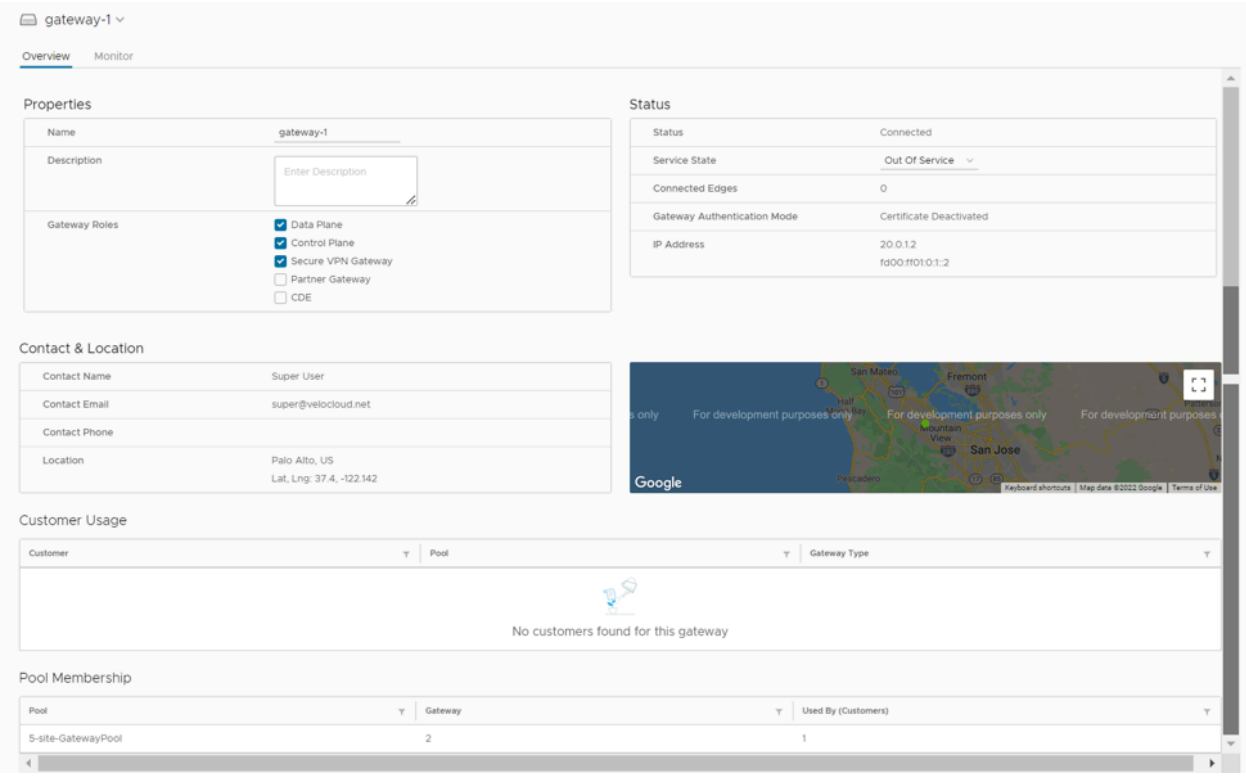
3. Select **Map Distribution** to expand and view the locations of the Gateways in the Map.
4. Users can also click the arrows before each Gateway's name to view additional details.

   The page displays the following details:

   - `Name` - Name of the Gateways.
   - `Status` - Current status of the Gateways. The status may be one of the following: Connected, Degraded, Never Activated, Not in Use, Offline, Out of Service, or Quiesced.
   - `CPU` - Percentage of CPU utilization by the Gateways.
   - `Memory` - Percentage of memory utilization by the Gateways.
   - `Edges` - Number of Edges connected to the Gateways.
   - `Service State` - Service state of the Gateways. The state may be one of the following: Historical, In Service, Out of Service, Pending Service, or Quiesced.
   - `IP Address` - The IP Address of the Gateways.
   - `Location` - Location of the Gateways.
5. In the **Search** field, enter a term to search for specific details. Click the Filter icon to filter the view by a specific criterion.
6. Select the **CSV** option to download a report of the Gateways in the CSV format.

7. Click the Gateway link to view the details of the selected Gateway.

Figure 16-19: View Selected Gateway Details

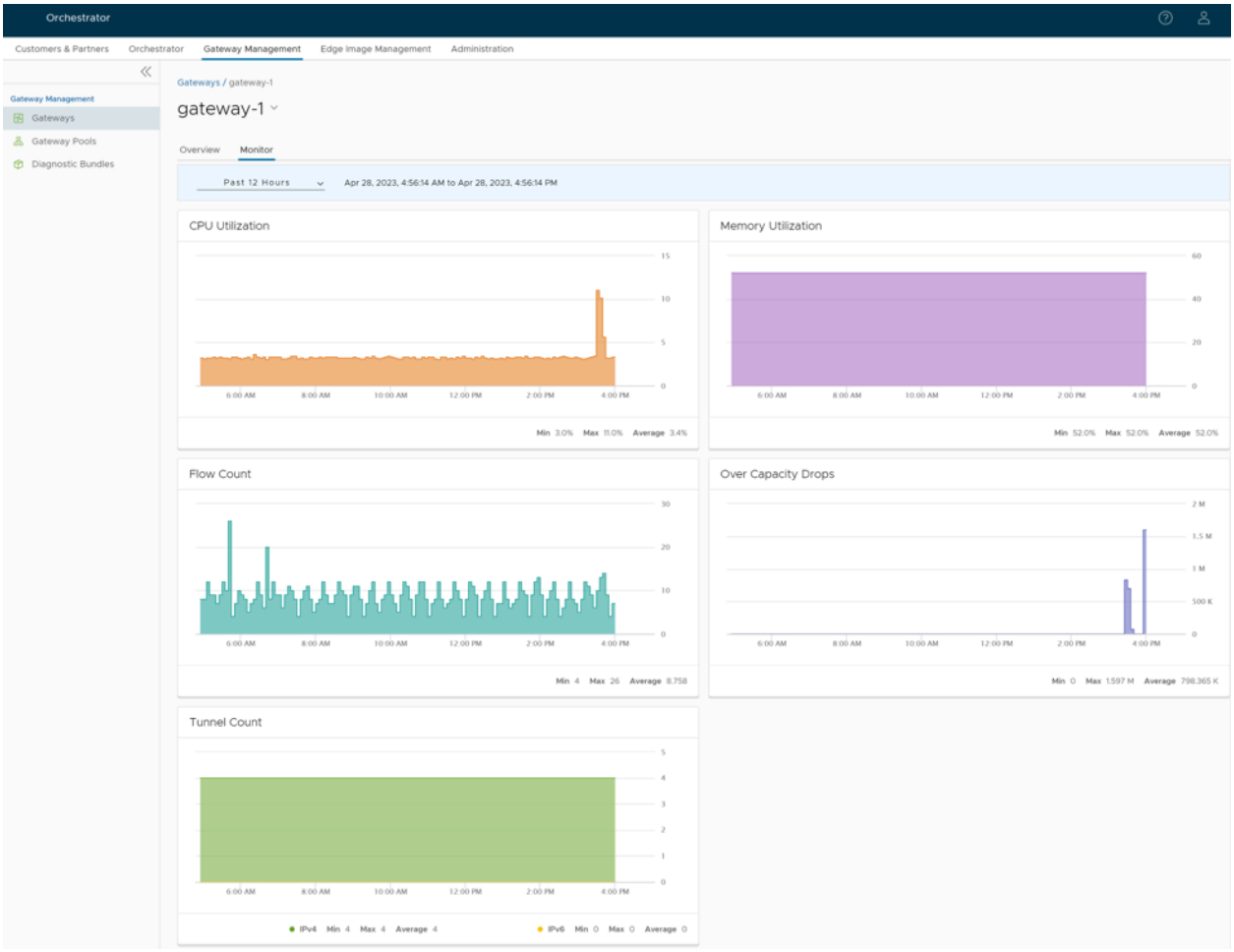


The **Overview** tab displays the properties, status, location, customer usage, and Gateway Pool of the selected Gateway.

Note: On the **Overview** tab, users can modify the **Name** and **Description** of the selected Gateway, and choose a different **Service State**. To configure the other options, navigate to the **Gateways** page in the **Operator** portal.

8. Click the **Monitor** tab to view the usage details of the selected Gateways.

Figure 16-20: View Selected Gateway Usage Details



At the top of the page, select a specific time period to view Gateway details for that period.

The page displays a graphical representation of usage details of the following parameters for the period of the selected time duration, along with the minimum, maximum, and average values:

- `CPU Percentage` - Percentage of CPU usage.
- `Memory Usage` - Percentage of memory usage.
- `Flow Counts` - Count of traffic flow.
- `Over Capacity Drops` - Total number of packets dropped due to over capacity since the last sync interval. Occasional drops are expected, typically due to a large traffic surge. However, a consistent increase in drops usually indicates a Gateway capacity issue.
- `Tunnel Count` - Count of tunnel sessions for both the IPv4 and IPv6 addresses.

Hover over the graphs to view additional details.

16.3 VeloCloud Gateway Migration

The VeloCloud Orchestrator offers self-service migration functionality, enabling migration from an existing Gateway to a new Gateway without requiring your Operator's support.

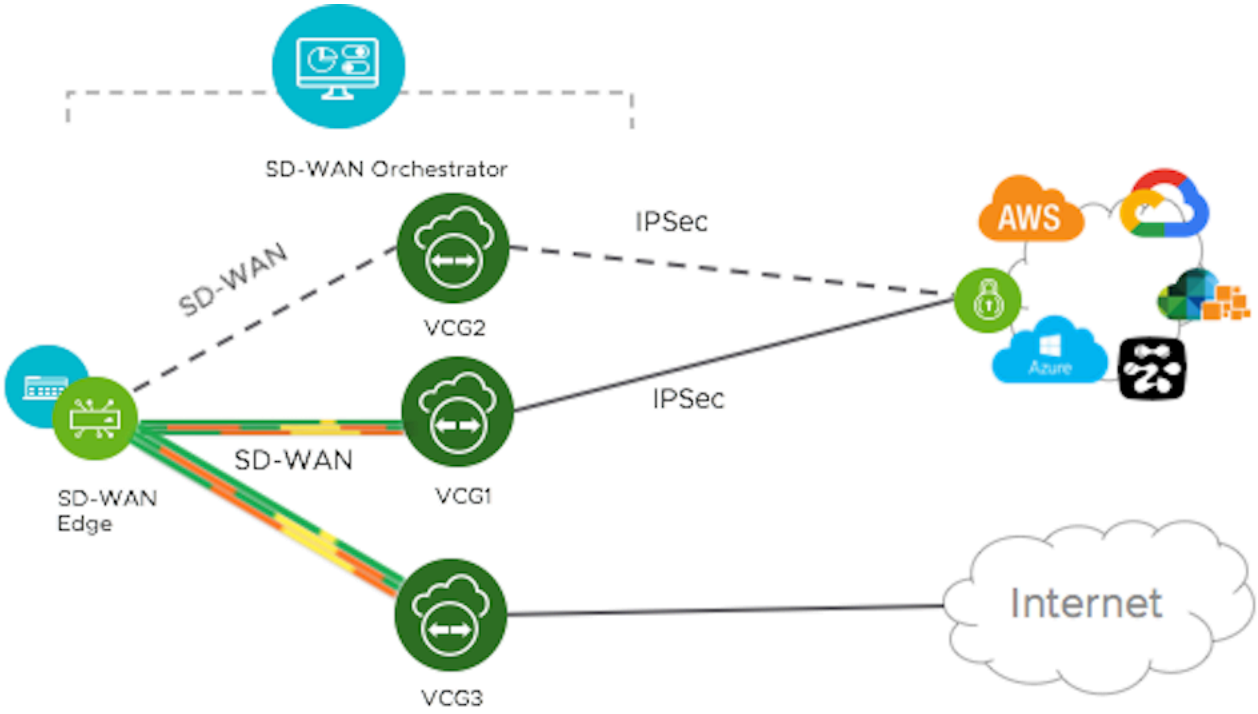
The following scenarios require Gateway migration:

- Achieving operational efficiency.
- Decommissioning old Gateways.

Gateway configurations define specific roles. For example, a Gateway with a data-plane role forwards data-plane traffic from source to destination. Similarly, a Gateway with a Control Plane role is referred to as a Super Gateway and is assigned to an Enterprise. The Super Gateway establishes connections with all Edges within the Enterprise. Additionally, a Gateway with the Secure Virtual Private Network (VPN) role establishes an Internet Protocol Security (IPSec) tunnel to a Non SD-WAN Destination (NSD). The migration steps may vary based on the role configured for the Gateway. For additional information about the Gateway roles, see the Configure Gateways" section.

The following figure illustrates the migration process of the Secure VPN Gateway:

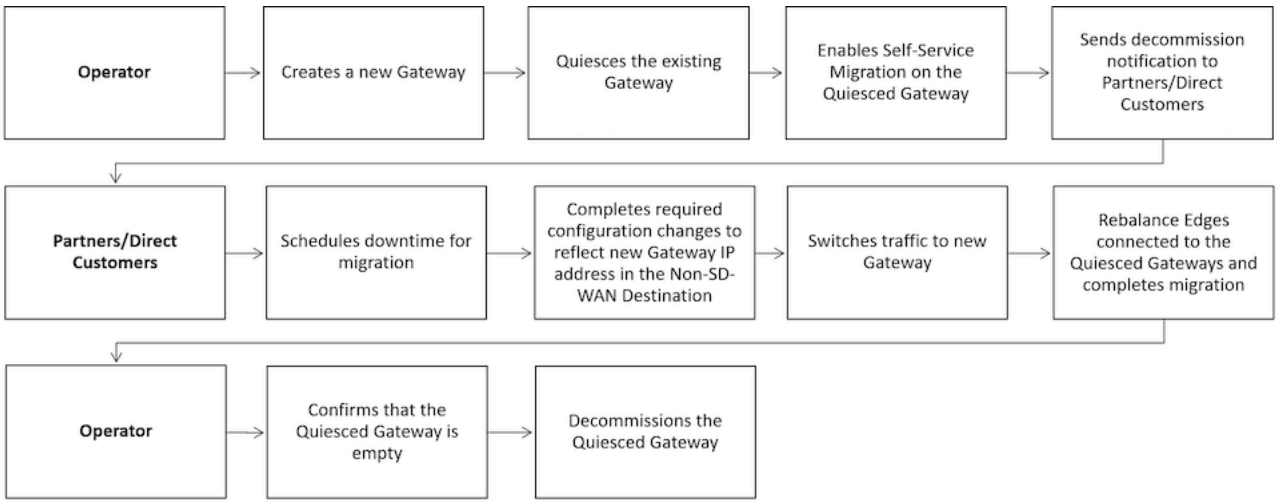
Figure 16-21: Secure VPN Gateway Migration Process



In this example, a VeloCloud Edge connects to an NSD through a Secure VPN Gateway, VCG1. The Orchestrator currently flags VCG1 for decommissioning. Before decommissioning, the administrator creates a new Gateway, VCG2, and assigns VCG2 the same role and attaches it to the same Gateway pool as VCG1, allowing VCG2 to replace the original Gateway. The administrator then changes VCG1's service state to "Quiesced," preventing the system from adding new tunnels or NSDs to VCG1. However, VCG1 retains its existing assignments. After the administrator updates the VCG2 IP address configuration in the NSD, VCG2 establishes an IPSec tunnel to the NSD and switches the traffic from VCG1 to VCG2. The administrator decommissions VCG1 after confirming it contains no remaining sessions.

Following is the high-level workflow of Secure VPN Gateway migration based on the User roles:

Figure 16-22: User Roles Secure VPN Gateway Migration - Workflow



See the following topics:

- Limitations of VeloCloud Gateway Migration
- Quiesce Gateways
- Decommission Quiesced Gateways

16.3.1 Limitations of VeloCloud Gateway Migration

Keep in mind the following limitations when migrating Gateways:

- Partner Gateways do not support self-service migration.
- There will be a minimum service disruption based on the time taken to switch Non SD-WAN Destinations (NSDs) from the quiesced Gateway to the new Gateway and to rebalance the Edges connected to the quiesced Gateway.
- If an NSD uses redundant Gateways and the administrator quiesces one Gateway, the remaining redundant Gateway cannot replace it.
- During self-service migration of a quiesced Gateway, the replacement Gateway must have the same Gateway Authentication mode as the quiesced Gateway.
- When a customer deploys an NSD via Gateway with Border Gateway Protocol (BGP) enabled, the Self-Service Gateway Migration feature does not migrate BGP configurations to the new Gateway. Consequently, the system drops all BGP sessions after the migration completes.

  In this scenario, the existing Gateway assigned to the NSD is in a quiesced state and requires migration to another Gateway. The customer then navigates to **Service Settings** > **Gateway Migration** on the Orchestrator and initiates the **Gateway Migration** process to move their NSD to a different Gateway. Post-migration, the new Gateway fails to populate the BGP Local ASN and Router ID fields, preventing NSD BGP sessions from establishing and causing the loss of all routes. Traffic remains disrupted until the administrator manually recreates all BGP settings.

This is a Day 1 issue, and while the **Gateway Migration** feature accounts for many critical NSD settings, the NSD's BGP settings that are not accounted for, and their loss post-migration, are an expected behavior.

Workaround: Gateway migration should be done only during a maintenance window. Before the migration, the user should document all BGP settings and manually reconfigure them after the migration to minimize impact on customer users.

16.3.2 Quiesce Gateways

When users choose to decommission a Gateway, ensure the Gateway is set to the Quiesced state so that no new tunnels or NSDs can be configured on it. Ensure that users have the Operator Super User role to quiesce Gateways.

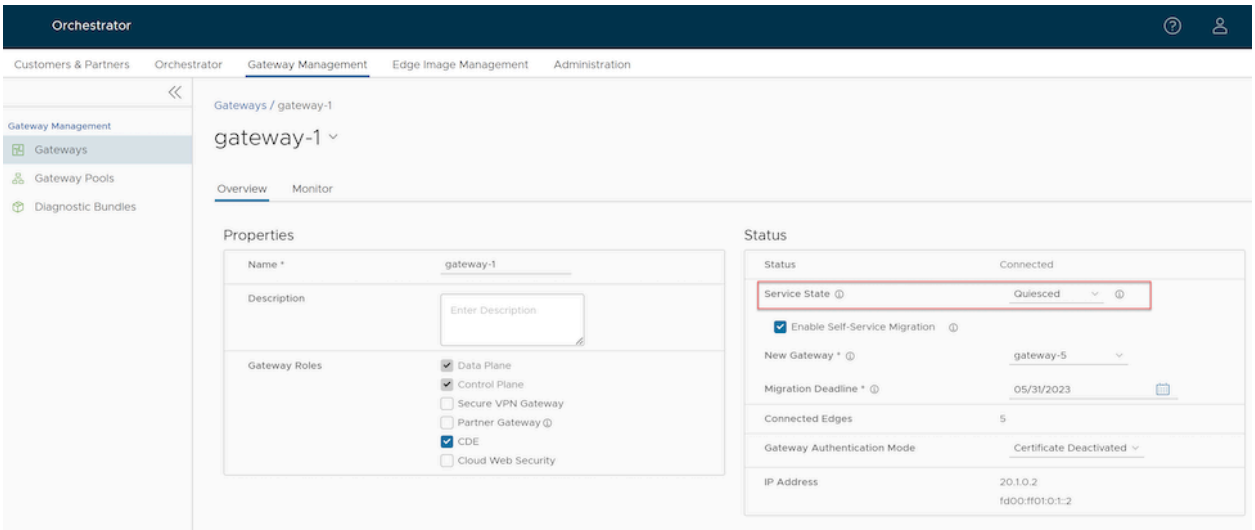
Before quiescing the existing Gateway, ensure that users create a new Gateway as a replacement. Assign the new Gateway with the same role and attach it to the same Gateway pool as the existing Gateway. For instructions, see the Manage Gateway Pools and Gateways section. Review the VeloCloud Gateway Migration- Limitations before proceeding with Gateway quiescing.

Note: Arista recommends that users select the self-service migration feature for NSD Gateway migration.

To quiesce the Gateway and enable self-service migration:

1. In the **Operator** portal, go to **Gateway Management**.
   The **Gateway** page lists the available Gateways.
2. Select the Gateway link that the user wants to quiesce.
   The Gateway details appear on the **Overview** tab.

Figure 16-23: Configure Quiesce Gateway



3. In the **Status** section, from the **Service State** drop-down menu, select **Quiesced**.
4. Select the **Enable Self-Service Migration** checkbox.
5. From the **New Gateway** drop-down list, select the Gateway that users have created as a replacement for the Gateway that they are quiescing.

6. In the **Migration Deadline** date picker, select a date by which users want the Partners or direct customers to complete the migration. Ensure the date is within 60 days of the current date.
7. Click **Save Changes**.

On the **Gateways** page, users can see that the Gateway's **Service State** has changed to **Quiesced**.

Send decommission notification to impacted Partners and direct customers. The notification email includes the migration deadline and detailed instructions for migrating the Edges and NSDs from the quiesced Gateway to the new Gateway.

The system displays a notification icon for any customer or Partner that has one or more Gateways in a Quiesced service state. Additionally, the system marks Edges with a notification icon if they are currently connected to a quiesced Gateway, alerting users to potential path changes.

Note: Decommission notification email is sent only to direct customers and not to Partners' customers.

16.3.3 Decommission Quiesced Gateways

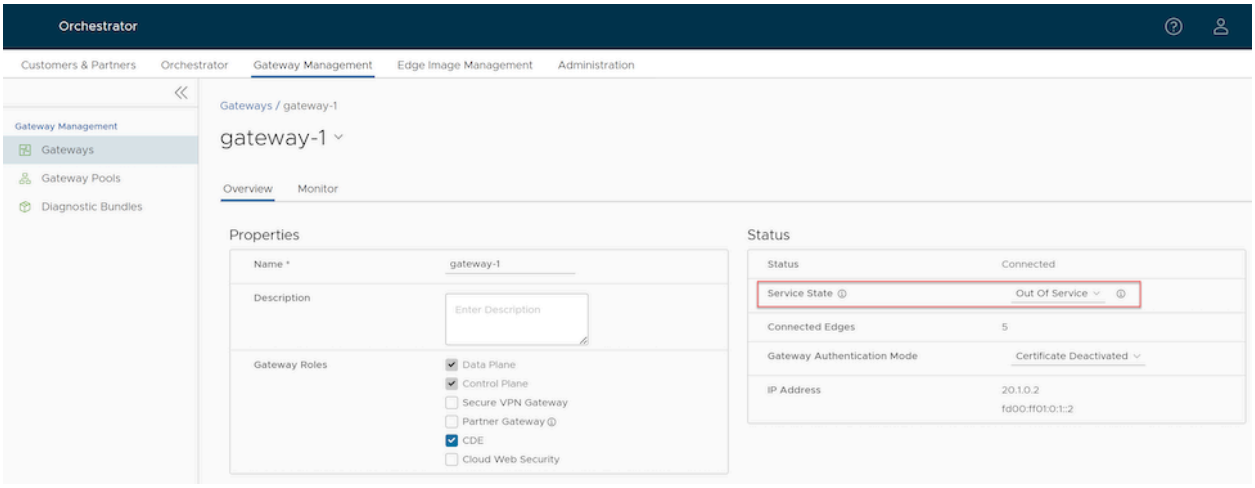
Before decommissioning the quiesced Gateways, ensure there are no Edges or NSDs connected to them.

If any Partners or direct customers have not yet migrated from the quiesced Gateways, follow up with them to ensure they migrate from the quiesced Gateways. Verify that the quiesced Gateway is empty and then decommission it.

To decommission a quiesced Gateway:

1. In the **Operator** portal, go to **Gateway Management**.
   The **Gateways** page lists the available Gateways.
2. Select the **Gateway** link the user wants to decommission.
   The Gateway details appear on the **Overview** tab.

Figure 16-24: Decommission Quiesced Gateways



3. From the **Service State** drop-down list, select **Out of Service**.
4. Click **Save Changes**.

Ensure to remove the Gateway from the Gateway pool and then delete the Gateway from Orchestrator.

16.4 Diagnostic Bundles for Gateways

Run diagnostics on Gateways to collect diagnostic bundles and packet capture files for troubleshooting purpose.

- Request Diagnostic Bundles for Gateways
- Request Packet Capture Bundle for Gateways

16.4.1 Request Diagnostic Bundles for Gateways

Diagnostic bundles allow users to collect all the configuration files and log files from a specific VeloCloud Gateway into a consolidated zipped file. Users can utilize the data within diagnostic bundles to troubleshoot Gateways.

The Operator Super user and Operator Admin user can create, manage, download, and delete diagnostic bundles for Gateways created by both Operator and Partner users.

Note: Operator Business Specialist users and Operator IT support users can only view the generated Diagnostic bundles and download the CSV file.

1. **Note:** To generate a new Diagnostic bundle:

   In the Orchestrator UI, click the **Gateway Management** tab and select **Diagnostic Bundles** in the left navigation pane.

   The **Diagnostic Bundles** page appears with the existing diagnostic bundles.
2. To generate a new Diagnostic bundle, select **Request Diagnostic Bundle**.
3. In the **Request Diagnostic Bundle** dialog, configure the following details and click **Submit**.

Figure 16-25: Request Diagnostic Bundle

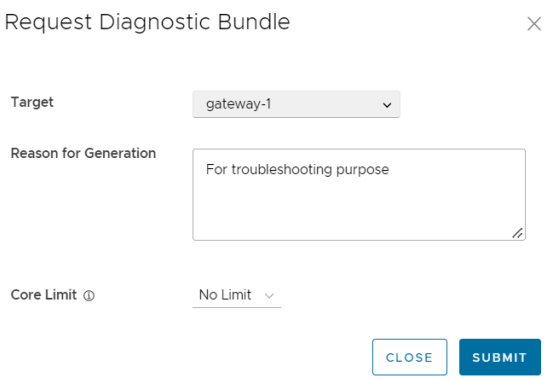


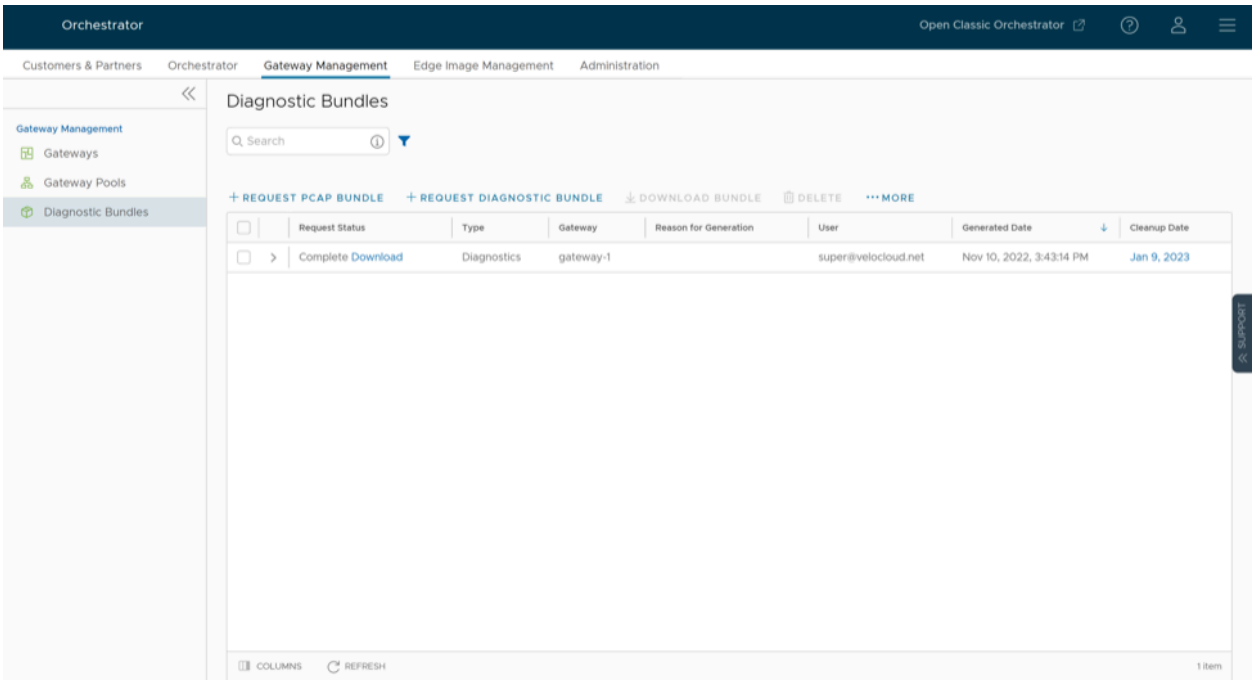
Table 63: Request Diagnostic Bundle Field Descriptions

Field	Description
Target	Select the target Gateway from the drop-down list. The system collects data from the selected Gateway.
Reason for Generation	Optionally, the user can enter the reason for generating the bundle.
Core Limit	Select a Core Limit value from the drop-down to reduce the size of the uploaded bundle when Internet connectivity is experiencing issues.

The **Diagnostic Bundles** page displays details of the bundle being generated, including its status.

To search a specific diagnostic bundle, enter a relevant search text in the **Search** box. For advanced search, select the **filter** icon next to the **Search** box to filter the results by specific criteria.

Figure 16-26: Manage Diagnostic Bundles



Download Diagnostic Bundle

Users can download the generated Diagnostic bundles to troubleshoot an Edge.

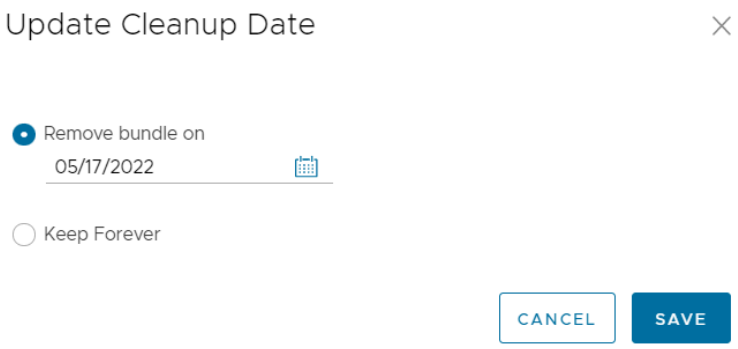
To download a generated bundle, click the link next to **Complete** in the **Request Status** column, or select the bundle, then click **Download Bundle**. The system downloads the bundle as a ZIP file.

Users can send the downloaded bundle to the Arista Support representative for debugging the data.

Delete Diagnostic Bundle

The completed bundles get deleted automatically on the date displayed in the **Cleanup Date** column. Users can click the link to the **Cleanup Date** or choose the bundle, then select **More** > **Update Cleanup Date** to modify the date.

Figure 16-27: Update Cleanup Date



In the **Update Cleanup Date** dialog, users can choose the specific date when the system will delete the selected bundle. Setting this date allows users to manage storage effectively by ensuring that temporary diagnostic files do not persist longer than necessary for investigation.

If the user wants to retain the bundle, select the **Keep Forever** checkbox to prevent it from being automatically deleted.

To delete a bundle manually, select the bundle and click **Delete**.

16.4.2 Request Packet Capture Bundle for Gateways

The Packet Capture bundle captures real-time network traffic from the user's network. Users can utilize these files to analyze network characteristics, such as latency, jitter, or protocol errors, providing the granular visibility needed to solve complex connectivity issues. Users can utilize the data to debug network traffic and determine network status.

The Operator Super user and Operator Admin user can create, manage, download, and delete Packet Capture (PCAP) bundles for Gateways created by both Operator and Partner users.

Note: Operator Business Specialist users and Operator IT support users can only view the generated PCAP bundles and download the CSV file.

To generate a PCAP bundle:

1. In the **Operator** portal, select the **Gateway Management** tab and select **Diagnostic Bundles** in the left navigation pane.

   The **Diagnostic Bundles** page appears with the existing diagnostic bundles.
2. To generate a new PCAP bundle, select **Request PCAP Bundle**.

3. In the **Request PCAP Bundle** dialog, configure the following details and click **Generate**.

Figure 16-28: Request PCAP Bundle

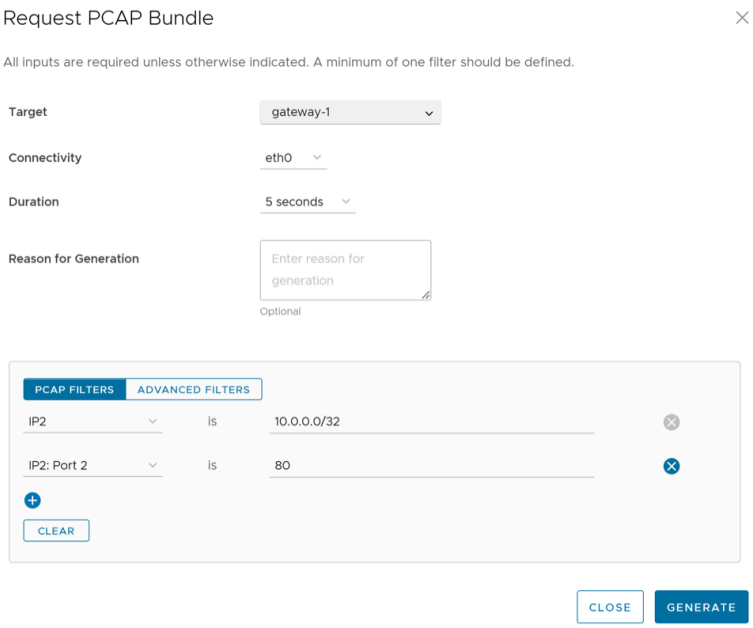


Table 64: Request PCAP Bundle Field Descriptions

Field	Description
Target	Choose the target Gateway from the drop-down list. The system collects the packets from the selected Gateway.
Connectivity	Choose an interface or an Edge ID from the drop-down list. The system collects the packets from the selected interface or Edge associated with the Gateway.
Duration	Choose the time in seconds. The system collects the packets for the selected duration. The default value is 5 seconds.
Reason for Generation	The user can optionally enter the reason for generating the bundle.
PCAP Filters	Users can define PCAP filters to control exactly which packet data the system generates by selecting the following options: • **IP1**- Enter an IPv4 address, or an IPv6 address, or a Subnet mask. • **IP2**- Enter an IPv4 address, or an IPv6 address, or a Subnet mask. • **IP1:Port1**- Enter a Port ID associated with IP1. • **IP2:Port2**- Enter a Port ID associated with IP2. • **Protocol**- Select a protocol from the list. **Note:** If users choose to utilize the PCAP filtering capability, they must define at least one filter.
Advanced Filters	Users can define free-form filters to control which PCAP data the system generates precisely.

The **Diagnostic Bundles** page displays details of the PCAP bundle being generated, including its status.

4. To download a generated bundle, click the link next to **Complete** in the **Request Status** column or select the bundle and click **Download Bundle**. The system downloads the bundle as a ZIP file.

5. The system automatically deletes the completed bundles on the date displayed in the **Cleanup Date** column. Users can click the link to the **Cleanup Date** or choose the bundle, then select **More** > **Update Cleanup Date** to modify the date.
6. To delete a bundle manually, select the bundle, then click **Delete**.

Chapter 17

Platform and Modem Firmware and Factory Images

Operators can upload, modify, or delete Platform and Modem Firmware images for specific Edge devices and Factory images for all physical VeloCloud Edge devices from the Orchestrator.

1. In the **Operator** portal, select **Edge Image Management**.
2. To upload a Firmware image, select **Firmware**. To upload a Software image, select **Software**.

> **Note:** Operators can upload, modify, or delete the following firmware and factory images:
>
> - Firmware Platform images for 6x0, 7x0, and 3x00 (3400/3800/3810) Edge device models
> - Firmware Modem images for 510-LTE (Edge 510LTE-AE, Edge 510LTE-AP) and 610-LTE (Edge 610LTE-AM, Edge 61LTE-RW)
> - Factory images for all physical VeloCloud Edge devices

For additional information about uploading and managing Firmware images, see the topic Manage Operator Profiles.

3. In the appropriate screen, select **+Upload Image** and select an image file in ZIP format with a file size less than 200MB to upload from your local storage.

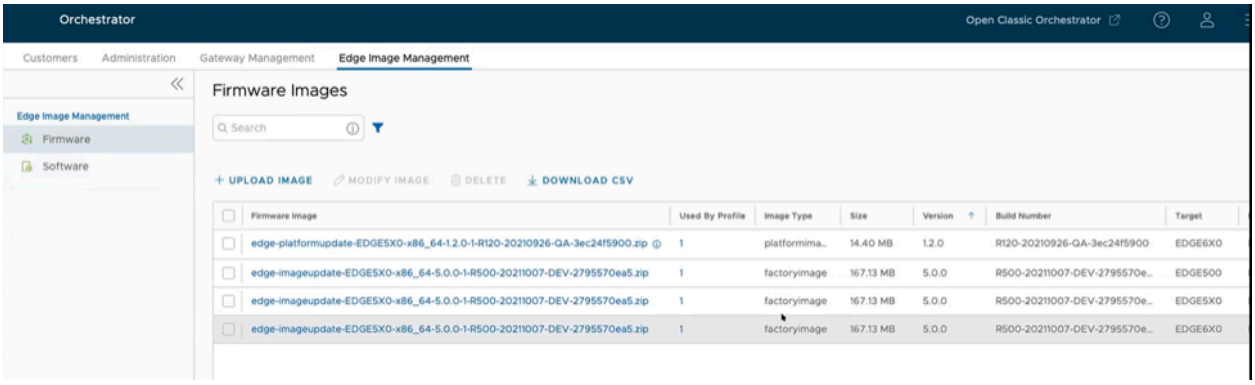
> **Note:** Update the software version first. Then, after completion, update the firmware, Platform or Modem, and the factory default. Do not update the software version, the firmware, and the factory default at the same time.

4. After attaching the file successfully, select **Done** in the **File Upload** dialog.

The Orchestrator UI validates the package and uploads it to the portal. You can upload multiple Firmware and Software images to the portal. The uploaded packages display on the appropriate page, **Firmware Images or Software Images**, based on your selected image type.

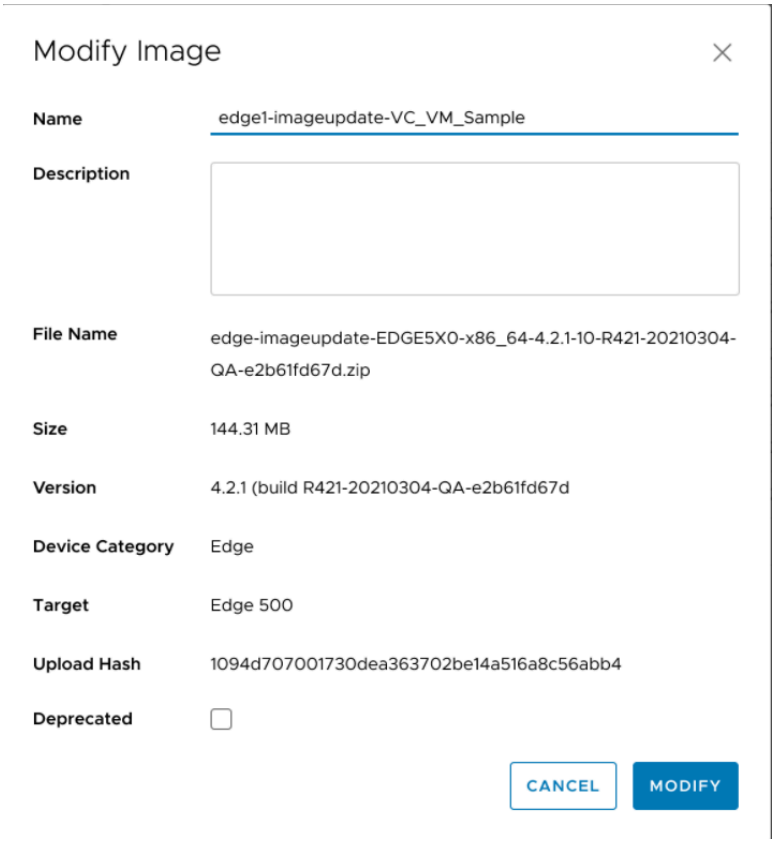
> **Note:** When selecting **Firmware** , note the **Image Type** column which indicates if the image is Platform Firmware or Factory Default.

Figure 17-1: Firmware Images



5. To modify a Firmware or Software image, select an image from the appropriate page, **Firmware** or **Software**, and then select **Modify Image**. **Modify Image** appears.

Figure 17-2: Modify Image



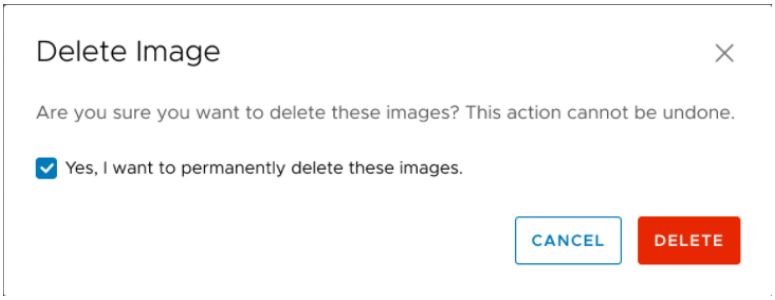
6. Update the Name and Description of the Firmware or Software image package, if needed.
7. If necessary, select **Deprecated** to deprecate the Firmware or Software image, and then select **Modify**. The deprecated Firmware or Software image flags and appears in the respective page, **Firmware Images** or **Software Images**.

> **Note:** Once the image deprecates, the image does not appear in the list of available firmware or software images, or versions assigned to Operator Profiles, or Customers or Edges.

> **Note:** The existing Operator Profiles with a deprecated image also flag to notify the user that the Firmware or Software version of the profile contains a deprecated software image.

8. To delete a package from the portal, select the image and select **Delete**.

Figure 17-3: Delete Image



To manage VeloCloud Edges within an Enterprise with a specific Software/Firmware Image, see the topic Manage Operator Profiles.

Chapter 18

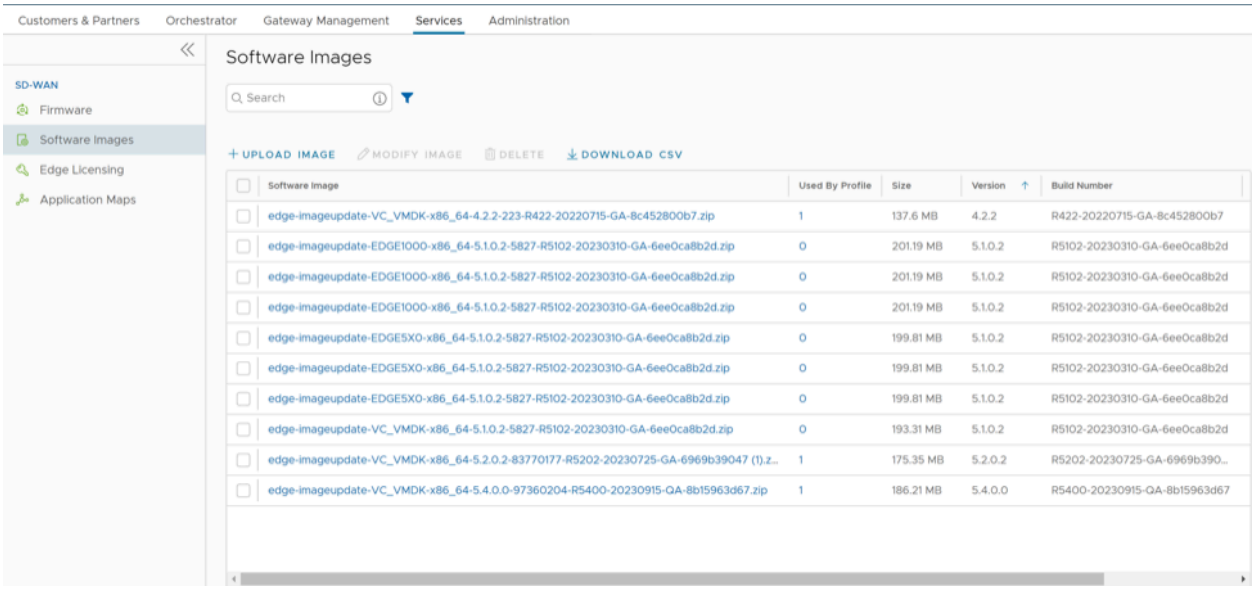
Software Images

The Orchestrator portal allows Operator Super Users and Operator Standard Admins to manage the Software Images for the associated Edges.

As an Operator Super User, you can upload a new software image, modify the existing software images, and delete a software image associated with the Edges.

1. To upload a new software image, in the **Operator** portal, select **Services**, then select **Software**.

   Figure 18-1: Manage Software Images



2. Select **Upload Image** and select an Image file, in ZIP format, to upload from your local storage. The Orchestrator validates the package and uploads it to the portal. You can upload multiple Software Images to the portal.
3. The uploaded packages display in the **Software Images** page.
4. To modify an uploaded software image, select the link to the image name. Or select the image, and then select **Modify Image**. The **Modify Image** appears.
5. You can update the Name and Description of the software image package, if needed.
6. Select **Deprecated** to deprecate the software image then select **OK**. Orchestrator flags the deprecated software image and it appears on the **Software Images** page.

   Note: Once deprecated, the image does not appear in the list of available software images or versions to assign to Operator Profiles, or Customers or Edges.

   Note: The existing Operator Profiles with a deprecated image also flag to notify the user that the software version of the profile contains a deprecated software image.

7. To delete a package from the portal, select the image then select **Delete**.

To upgrade the Edges within an Enterprise with a specific Software Image, see Manage Operator Profiles.

Chapter 19

Edge Licensing

Only Operators can enable the Edge Licensing and assign the licenses to a Partner user.

The Orchestrator activates the Edge Licensing feature by default. If the feature is inactive, contact the Operator.

To deactivate Edge Licensing, in the **Operator** portal, go to **Orchestrator** > **System Properties**, and set the value of the system property `session.options.enableEdgeLicensing` to **False**.

Edge Licenses provide the following components:

Table 65: Edge Licenses Components

Component	Supported Attributes
Bandwidth	10M, 30M, 50M, 100M, 200M, 350M, 500M, 750M, 1G, 2G, 5G, 10G
Editions	Standard, Enterprise, Premium
Region	North America, Europe Middle East and Africa, Latin America, Asia Pacific
Term	12 months, 36 months, 60 months

An Operator can assign different types of Edge licenses from the 324 types of licenses available with various combinations.

Apart from the above list, Arista offers a trial version of license with the following attributes:

Table 66: Trial Version Attributes

Component	Supported Attributes
Bandwidth	10 Gbps
Edition	POC
Region	North America, Europe Middle East and Africa, Asia Pacific and Latin America
Term	60 Months

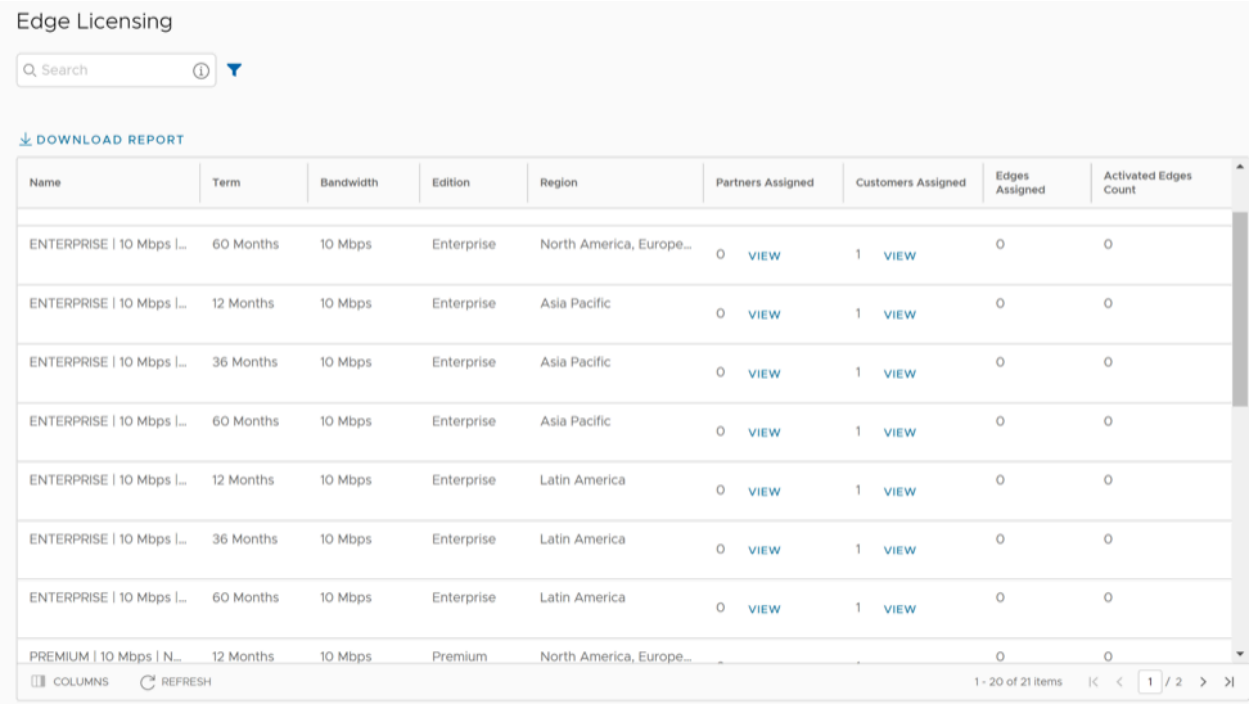
Note: The system allows assigning the **POC** license to a customer as a trial. An upgrade to any Edition remains available when required.

To access the Edge Licensing feature:

1. In the **Operator** portal, select **Services**, and then from the left menu, select **Edge Licensing**.

Note: Starting from the 5.4.0 release, **Edge Image Management** is renamed to **Services**.

Figure 19-1: Manage Edge Licensing



2. Users can view and update the following options on this page:

Table 67: Edge Licensing - Options and Descriptions

Option	Description
Search	Enter a term to search for a matching text across the table. Select the advanced search option to use filters to narrow down the search results.
Download Report	Select this option to download a report of the licenses, associated customers, and Edges in a CSV format.
Columns	Selecting this option enables the selection of specific columns to display in the table.
Refresh	Select this option to refresh the displayed list of licenses.

3. Selecting the **View** link under the **Partners assigned** column displays the Edge license details of the selected Partner.
4. Selecting the **View** link under the **Customers assigned** column displays the Edge license details of the selected Customer.

To assign Edge Licenses to new Partners, see Create a New Partner.

To manage and assign Edge Licenses to existing Partners, see Manage Edge Licenses for Partners.

To assign Edge Licenses to new Customers, see Create a New Customer.

To manage and assign Edge Licenses to existing Customers, see Manage Edge Licenses for Customers.

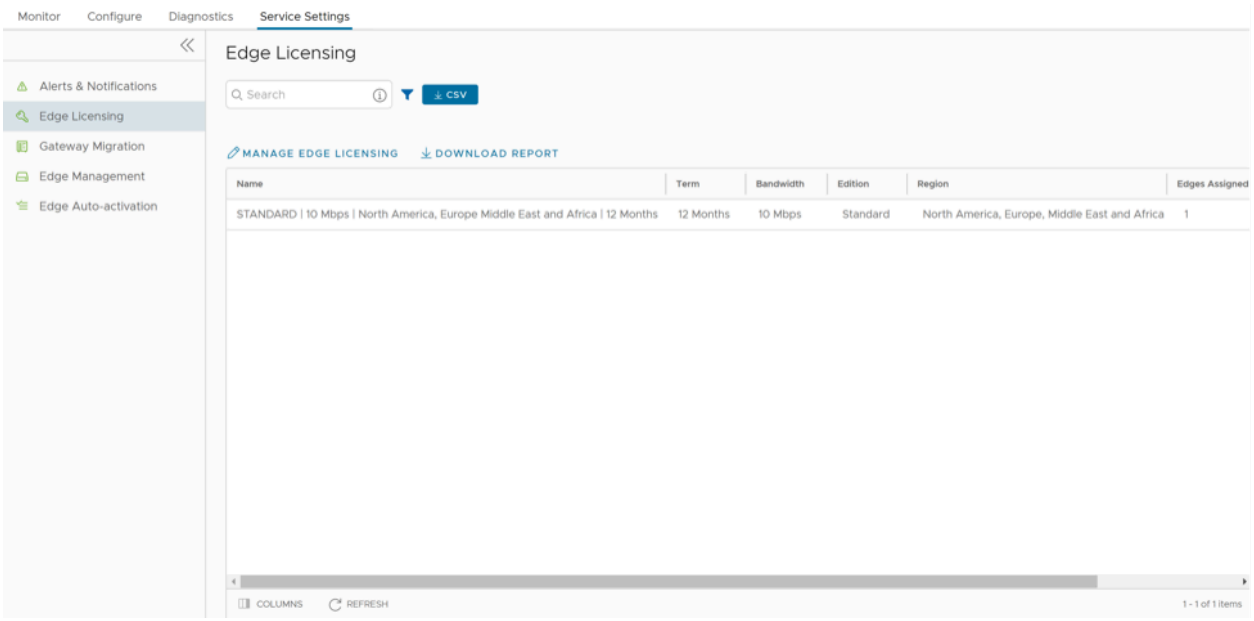
19.1 Manage Edge Licenses for Partners

An Operator can manage the Edge Licenses and assign them to Partners.

Perform the following steps to manage and assign Edge Licenses to existing Partners. To assign Edge Licenses to new Partners, see Create a New Partner.

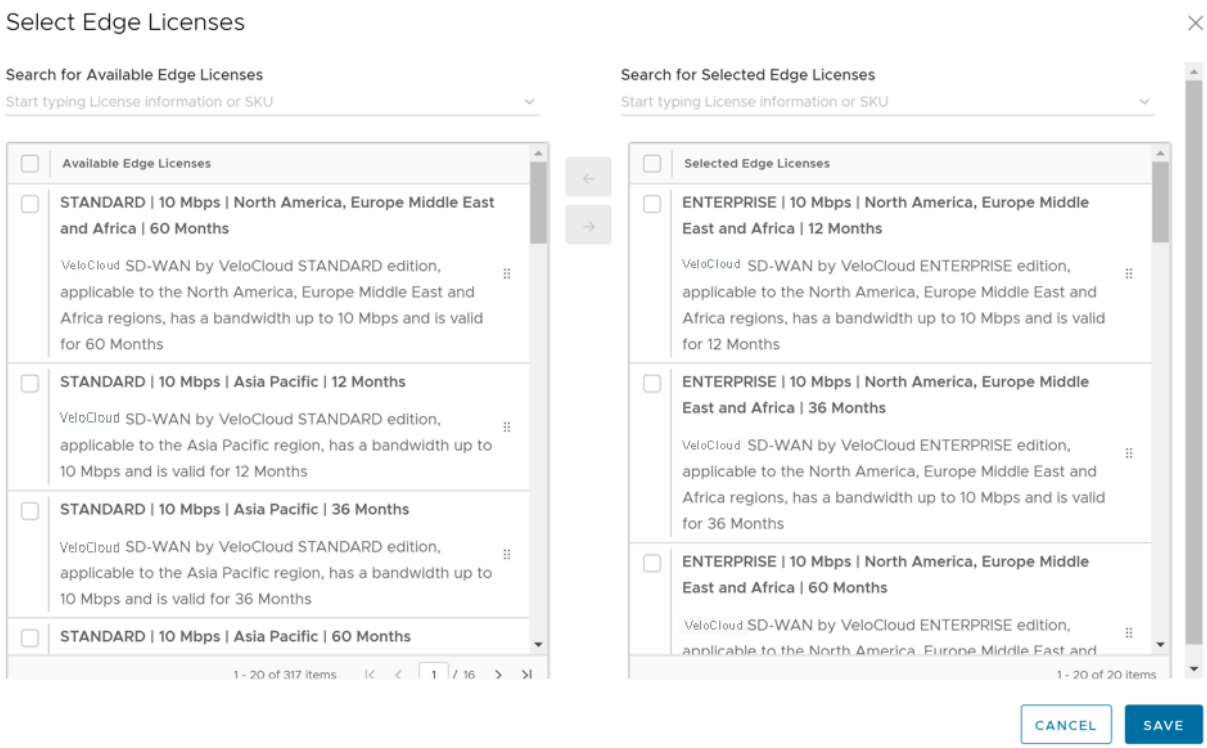
1. In the **Operator** portal, select **Manage Partners**.
2. Select the Partner name link to navigate to the **Partner** portal.
3. In the **Partner** portal, select **Edge Management**, and then from the left menu, select **Edge Licensing**.

Figure 19-2: Manage Edge Licensing for Partners



4. Select **Manage Edge Licensing**.

Figure 19-3: Select Edge Licenses for Partners



5. In the **Select Edge Licenses** window, choose the relevant licenses based on Bandwidth, Term, Edition, and Region, and then move them to the **Selected Edge Licenses** pane.
6. Select **Save**.

   The **Edge Licensing** window displays the selected licenses.
7. Select **Download Report** to generate a report of the licenses along with the associated customers and Edges in a CSV format.

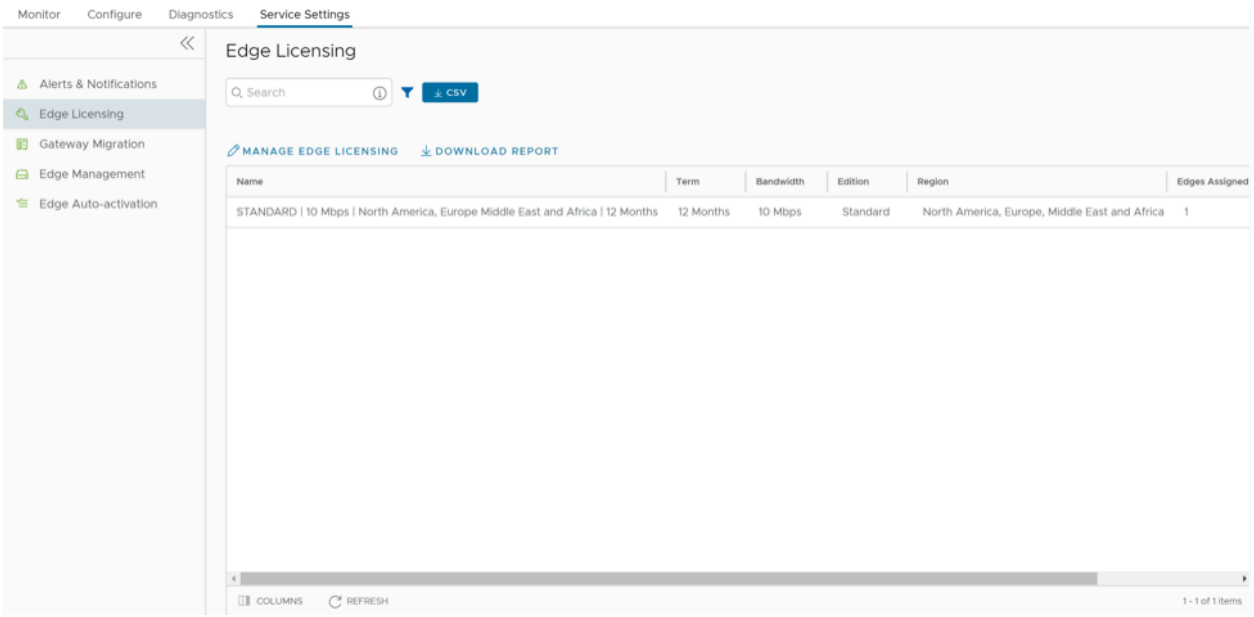
19.2 Manage Edge Licenses for Customers

An Operator can manage Edge Licenses and assign them to Customers.

1. In the **Operator** portal, select **Manage Customers**.
2. Select the Customer name link to navigate to the **Enterprise** portal.

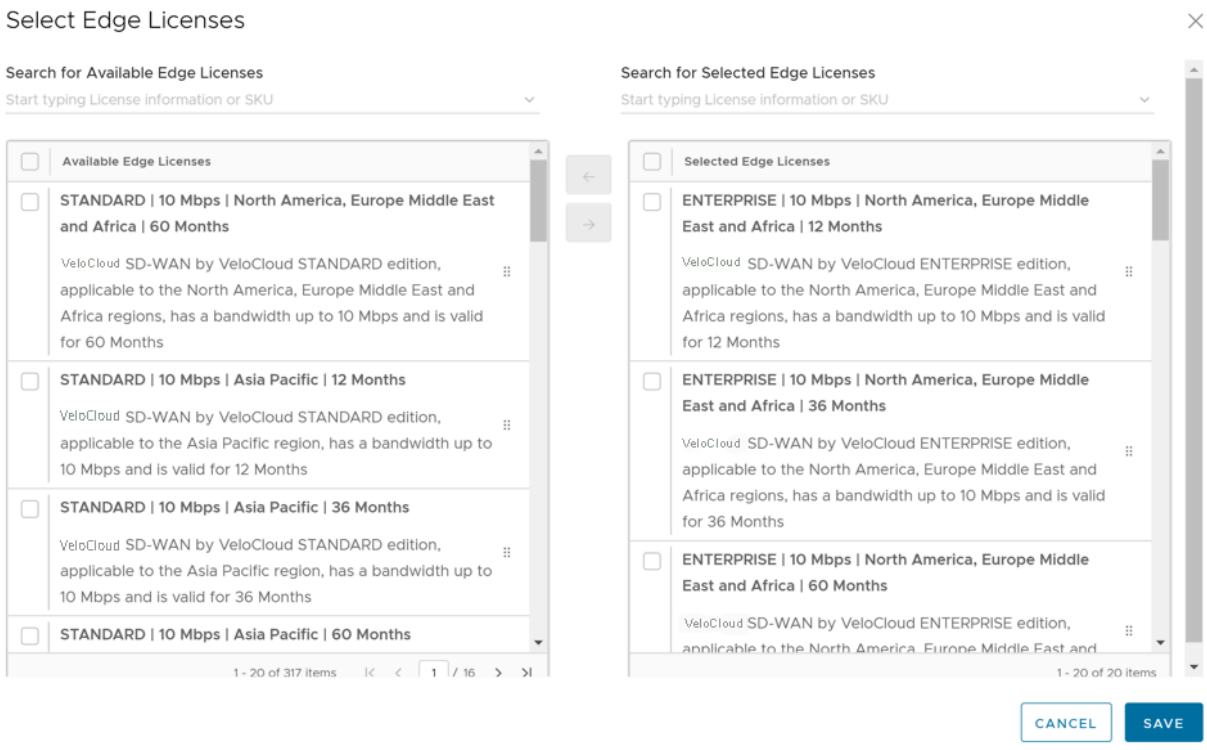
3. In the **Enterprise** portal, select **Service Settings** > **Edge Licensing**.

Figure 19-4: Manage Edge Licensing for Customers



4. Select **Manage Edge Licensing**.

Figure 19-5: Select Edge Licenses for Customers



5. In the **Select Edge Licenses** window, choose the relevant licenses based on Bandwidth, Term, Edition, Region, and then move them to the **Selected Edge Licenses** pane.

> **Note:** Apart from the existing licenses, Arista offers a trial version of license with the Edition as **POC**. A **POC** license selection disables all other license options.

6. Select **Save**.
   The **Edge Licensing** window displays the selected licenses.

   > **Note:** For a **POC** license, select **Upgrade Edge License** to upgrade the license to the next level. Choose either **Standard**, **Enterprise**, or **Premium Edition** from the list. The Orchestrator prohibits downgrading a license type to a previous Edition.

7. Select **Report** to generate a report of the licenses and the associated VeloCloud Edges in a CSV format.

When creating an Edge, choose and assign an Edge License from the drop-down menu.

To assign a license to an existing Edge:

- In the **SD-WAN** service of the **Enterprise** portal, select **Configure** > **Edges**.
- To assign license to each Edge, select the Edge link, and then select the License in the **Properties** section of the **Edge Overview** page. Alternatively, select the Edge, and then select **Assign Edge License** to assign the license.
- To assign a license to multiple Edges, select the appropriate Edges, select **Assign Edge License**, and then select the License.

Chapter 20

Application Maps

The Application Maps have JSON files consisting of various Applications with definitions used while creating Business Policies.

From the **Operator** portal, select **Services**, and then select **Application Maps**. The following screen displays:

Figure 20-1: Manage Application Maps

Note: Starting from the 5.4.0 release, **Edge Image Management** is renamed to **Services**.

You can perform the following actions on this page:

- Upload Application Map
- Clone Application Map
- Refresh Application Map
- Push Application Map
- Edit Application Map
- Delete Application Map

Upload Application Map

VeloCloud SD-WAN provides an initial Application Map with possible applications. You can also upload your JSON file with Applications to use in Business Policies.

- To upload a map file, select **Upload**.
- In **File Upload**, you can either drag and drop, or browse and select the **Application Map** file to upload.
- Select **Done**. The file uploads after validating the content.

- The **Application Map** file has a JSON format and you can customize the applications as per your requirements. The following example illustrates a customized JSON file for the application BitTorrent.

```
{
  "id": 15,
  "name": "APP_BITTORRENT",
  "displayName": "bittorrent",
  "class": 14,
  "description": "BitTorrent is a peer-to-peer protocol. [Note: bittorrent is also known as
 kadmelia.]",
  "knownIpPortMapping": {},
  "protocolPortMapping": {},
  "doNotSlowLearn": 1,
  "mustNotUseGateway": 1
}
```

Clone Application Map

You can create a new **Application Map** by cloning an existing **Application Map**.

- Select an existing **Application Map**, and then select **Clone**.
- On the **Clone Application Map**, enter a new name and description for the Application.
- Select **Clone**.

Refresh Application Map

You can update the Application definitions, managed by third party SaaS providers, listed in the Application Map.

- Select one or more **Application Maps**, and then select **Refresh**. **Refresh Application Maps** appears which lists the details of the selected Application Map(s) and Profile Count associated with the selected Application Map(s).
- Select **Refresh** to refresh the selected Application Map(s).

Note: The Application map Refresh operation serves to update application definitions managed by third party SaaS providers, for example Microsoft Office365®. It does not push those updates to associated Edges. After **Refresh**, use **Push** to update Edges assigned to a selected application map.

Push Application Map

You can push the latest updates of the Application definitions available in **Application Maps** to the associated VeloCloud Edges.

- Select an **Application Map**, and then select **Push**.
- Select **Push to Edges** to update the latest Application definitions available in the selected Application Map.

Note: This option pushes the Application definitions only when any updates are available.

Important: When you change an application map and push those changes to the Edges from the Orchestrator, all Edge flows flush. This ensures all Edge flows apply the updated version of the application map. As a result, you should only push an update to a custom application map in a maintenance window to minimizes disruption from an Edge flow flush.

Note: On Hosted Orchestrators, the Cloud Operations team updates and pushes all application maps on the first Saturday of each month. The application map refresh operation serves to update application definitions managed by third-party SaaS providers, for example, Microsoft 365. Schedule updates and pushes to minimize the disruption to customer traffic as follows:

Table 68: Application Definitions by Region

Region	Local Time	UTC Time	Day of the Month
Asia Pacific	02:00	18:00 UTC	1st Saturday of the month
Europe	02:00	00:00 UTC	1st Saturday of the month
North America	02:00	08:00 UTC	1st Saturday of the month

As noted earlier, an application map refresh and push flushes all flows for the Edges associated with that map and customers should anticipate this in the monthly maintenance window when performed.

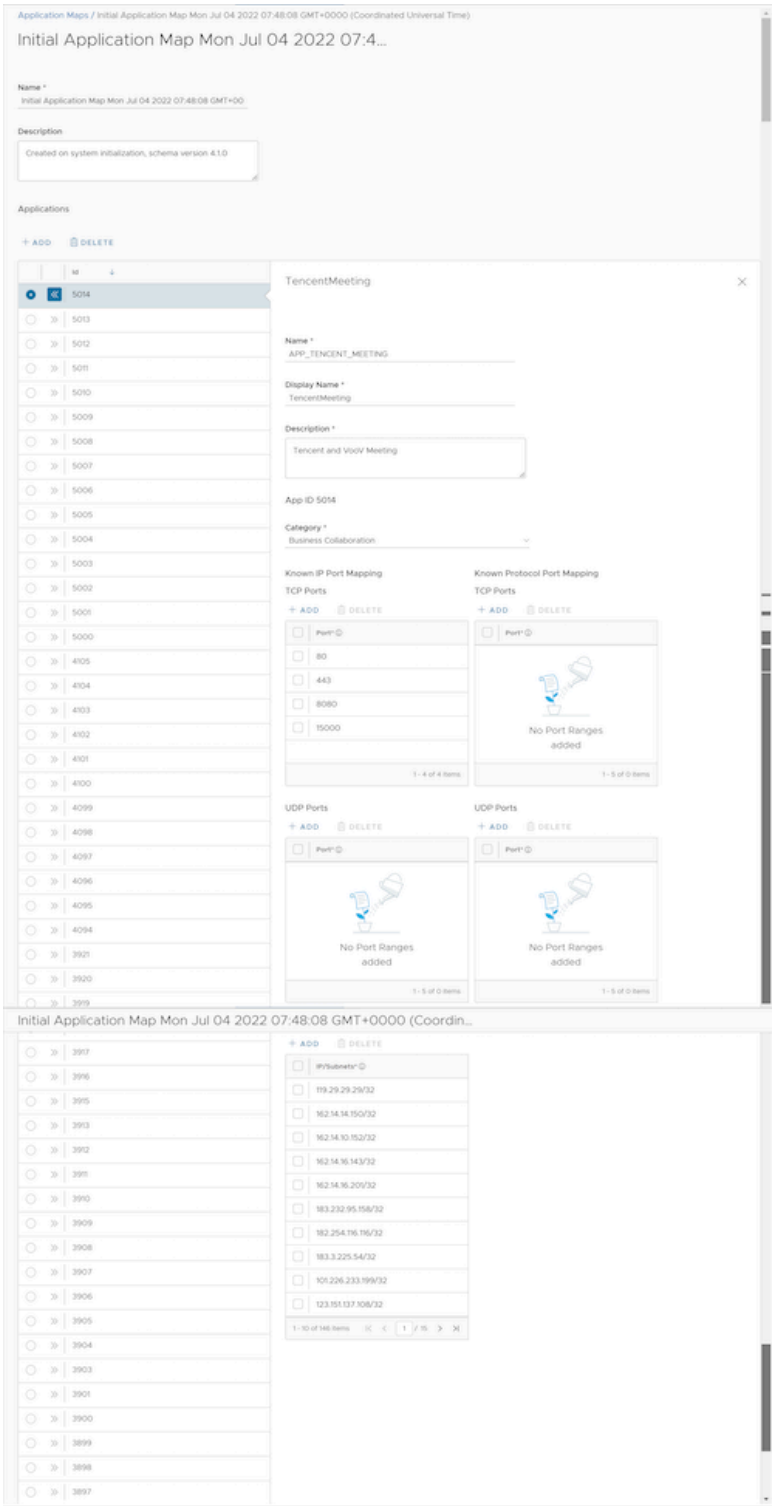
Edit Application Map

You can add or update the application details available in the existing Application Maps.

- Select an **Application Map**, and then select **More** > **Edit** to edit the associated Application.
- Select **Add** to add a new application along with the ID. Update details like **Name**, **Display Name**, **Description**, **Category**, **TCP Ports**, **UDP Ports**, and **IP/Subnets**.
- Select **Delete** to delete the selected application.

- Select **Save Changes** to save the entered details.

Figure 20-2: Edit Application Map



Delete Application Map

You can delete a selected Application Map, but you cannot delete a map assigned to an Operator profile.

- Select an Application Map and then select **More** > **Delete**.
- Enter the **Number of Application maps selected** and select **Delete**.

Chapter 21

Edge Management

Edge Management feature allows users to configure general settings, authentication, and encryption for an Edge. It allows activation and deactivation of configuration updates for an Edge. Users can also select a default Software & Firmware Image.

1. In the **Operator** portal, on the **Monitor Customers** screen, select on a **Customer** name.
2. From the top menu, select **Service Settings**, and then from the left menu, select **Edge Management**.
3. Configure the following options, and then select **Save Changes**.

Figure 21-1: Edge Management

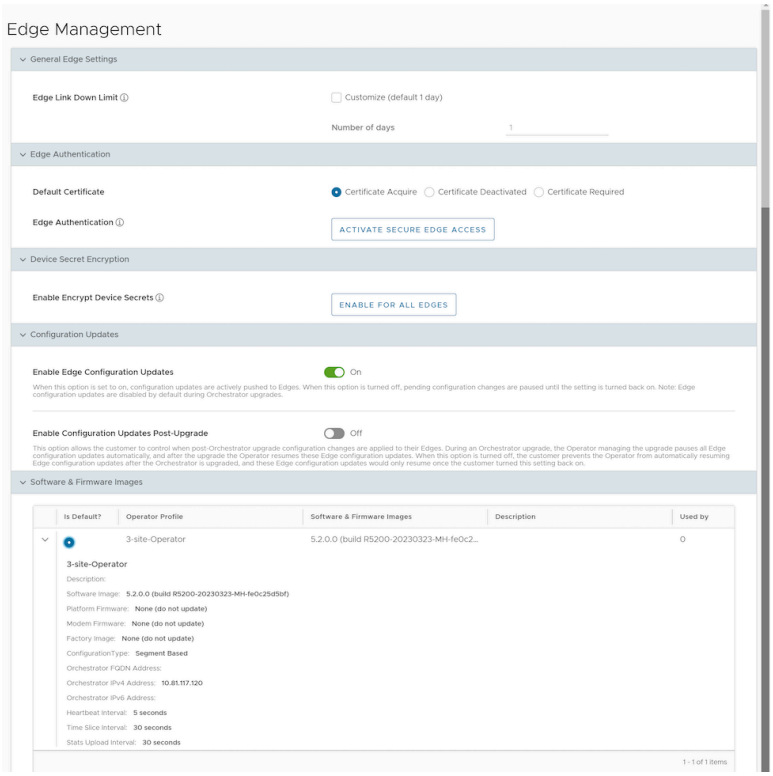


Table 69: Edge Management - Options and Descriptions

Option	Description
General Edge Settings	
Edge Link Down Limit	Set this value for each Edge by selecting the **Customize** checkbox. This overrides the value set through the system property `edge.link.show.limit.sec`.
Number of days	Enter a value in the range 1 to 365. The default value is 1.
Edge Authentication	
Default Certificate	Choose the default option to authenticate the Edges associated to the Customer. • **Certificate Acquire:** This option instructs the Edge to acquire a certificate from the certificate authority of the Orchestrator, by generating a key pair and sending a certificate signing request to the Orchestrator. Once acquired, the Edge uses the certificate for authentication to the Orchestrator and for the establishment of VCMP tunnels. **Note:** The Orchestrator allows updates to **Certificate Required** only after the certificate is acquired. • **Certificate Deactivated:** This option instructs the Edge to use a pre-shared key mode of authentication. • **Certificate Required:** This is the default option, and it instructs the Edge to use the PKI certificate. Operators can change the certificate renewal time window for Edges using system properties. For additional information, contact your Operator. **Note:** When selecting **Save Changes**, the Orchestrator prompts the users to confirm whether the selected Edge authentication setting applies to all impacted Edges or only the new Edges. By default, the Orchestrator selects the **Apply to all Edges** checkbox.
Edge Authentication	Select the **Activate Secure Edge Access** button to allow the user to access Edges using Password-based or Key-based authentication. Activate this option only once. The Orchestrator supports switching between Password-based and Key-based authentication an unlimited number of times. For additional details, see Configure User Account Details.
Device Secret Encryption	
Enable Encrypt Device Secrets	Select the **Enable For All Edges** button to activate device secret encryption for all the Edges in the current Enterprise. This action causes restart of all the Edges. However, activated Edges maintain their current status without disruption. **Note:** Activate this option for individual Edges at the time of creating a new Edge. For additional information, see the topic *Provision a New Edge* in the *Arista VeloCloud SD-WAN Administration Guide*.
Configuration Updates	
Disable Edge Configuration Updates	By default, the Orchestrator activates this option. This option enables active pushing of configuration updates to Edges. Slide the toggle button to turn it off.
Enable Configuration Updates Post-Upgrade	By default, the Orchestrator deactivates this option. This option allows users to control the timing of post-Orchestrator upgrade configuration changes for their Edges. Slide the toggle button to turn it on.

Software & Firmware Images

To view this section, an Operator user must follow the below steps:

1. Navigate to the **Global Settings** service of the **Enterprise** portal.

2. Go to **Customer Configuration** > **SD-WAN Configuration**.
3. Select the **Allow Customer to manage software** checkbox.

> **Note:** Only an Operator user can add, delete, or edit an image.

For additional information, see the topics Platform and Modem Firmware and Factory Images and Software Images.

Chapter 22

Access SD-WAN Edges Using Key-Based Authentication

This section discusses details about how to enable key-based authentication, add SSH keys, and access Edges more securely.

The Secure Shell (SSH) key-based authentication is a secure and robust authentication method to access VeloCloud Edges. It provides a strong, encrypted verification and communication process between users and Edges. The use of SSH keys bypasses the need to manually enter login credentials and automates the secure access to Edges.

Note:

- Both the Edge and the Orchestrator must be using Release 5.0.0 or later for this feature to be available.
- Users with Operator Business or Business Specialist account roles cannot access Edges using key-based authentication.

Perform the following tasks to access Edges using key-based authentication:

1. Configure privileges for a user to access Edges in a secure manner.

   Choose **Basic** access level for the user. Configure the access level when creating a new user and choose to modify it at a later point in time. Users must have the Superuser role to modify a user's access level. See User Management-Operator.
2. Generate a new pair of SSH keys or import an existing SSH key.

   See Add SSH Key.
3. Enable key-based authentication to access Edges.

   See Enable Secure Edge Access for an Enterprise Operator.

See the following topics:

- Revoke SSH Keys
- Secure Edge CLI Commands

22.1 Add SSH Key

When using key-based authentication to access Edges, the system generates a pair of SSH keys: Public and Private.

The system stores the public key in a database shared with the Edges and downloads the private key to the computer. Select this key along with the SSH username to access Edges. Users can generate only one SSH key pair at a time. To add a new SSH key pair, delete the existing one, and then generate a new one. If a previously generated private key is lost, users cannot recover it from the Orchestrator. In such cases, delete the key and then add a new key to gain access. For details about how to delete SSH keys, see Revoke SSH Keys.

Based on their roles, users can perform the following actions:

- All users, except users with Operator Business or Business Specialist account roles, can create and revoke SSH keys for themselves.
- Operator Superusers can manage SSH keys of other Operator users, Partner users, and Enterprise users, if the Partner user and Enterprise user have delegated user permissions to the Operator.
- Partner Superusers can manage SSH keys of other Partner users and Enterprise users, if the Enterprise user has delegated user permissions to the Partner.
- Enterprise Superusers can manage the SSH keys of all the users within that Enterprise.
- Superusers can only view and revoke the SSH keys for other users.

Note: Enterprise and Partners customers without SD-WAN service access will not be able to configure or view SSH key-related details.

To add an SSH key:

1. In the **Enterprise** portal, select the User icon that appears at the top-right side of the window.
   The **User Information** panel appears.
2. Select **Add SSH Key**.
   The **Add SSH Key** pop-up window appears.
3. Select one of the following options to add the SSH key:
   - **Generate Key**: Use this option to generate a new pair of public and private SSH keys. Note that the system automatically downloads the generated key. SSH key generation uses the `.pem` format as the default. When using a Windows operating system, convert the file format from `.pem` to `.ppk`, and then import the key. For instructions to convert `.pem` to `.ppk`, see https://puttygen.com/convert-pem-to-ppk.
   - **Import Key**: Use this option to paste or enter the public key if users already have a pair of SSH keys.
   - **Enter key**: Use this option to paste or enter the public key if users already have a pair of SSH keys.
4. In the **PassPhrase** field, choose to enter a unique passphrase to further safeguard the private key stored on the computer.

Note: This is an optional field and is available only if a user has selected the **Generate Key** option.

5. In the **Duration** drop-down menu, select the number of days by which the SSH key must expire.
6. Select **Add Key**.

Enable secure Edge access for the Enterprise and switch the authentication mode from Password-based to Key-based. See Enable Secure Edge Access for an Enterprise Operator.

22.2 Revoke SSH Keys

Users must have a Superuser role to delete the SSH keys for other users.

To revoke the SSH key:

1. In the **Enterprise** portal, select the User icon that appears at the top-right side of the window.
   The **User Information** panel appears.

2. Select **Revoke SSH Key**.

For Other Operator Users

To revoke the SSH keys of other Operator users:

1. In the **Operator** portal, go to **Orchestrator Authentication**.
2. In the **SSH Keys** area, select specific SSH usernames to initiate the deletion of their associated SSH keys.
3. Select **Actions** > **Revoke SSH Key**.

   The system deletes the SSH keys for a user in the following cases:

   - Changing the user role to **Operator Business** or **Business Specialist** prevents Edge access via key-based authentication.
   - Deleting a user from the Orchestrator.

     Note: Deleting or deactivating a user in an external SSO provider prevents them from accessing the Orchestrator. Only the explicit removal of the user from the Orchestrator deactivates the associated Secure Edge Access keys. Therefore, first delete the user from the IdP before deleting from the Orchestrator.

22.3 Enable Secure Edge Access for an Enterprise

After adding the SSH key, users must switch the authentication mode from Password-based (the default) to Key-based to access Edges using the SSH username and SSH key. The Orchestrator generates an SSH username simultaneously with each new user account.

To enable secure Edge access:

1. In the **SD-WAN** service of the **Enterprise** portal, go to **Service Settings** > **Edge Management**.
2. Select the **Enable Secure Edge Access** checkbox to allow the user to access Edges using Key-based authentication. Once activated, users cannot deactivate Secure Edge Access.

   Note: Only Operator users can enable Secure Edge Access for an Enterprise.

3. Select **Switch to Key-Based Authentication** and confirm the selection.

   Note: Users must have a Superuser role to switch the authentication mode.

Use the SSH keys to securely login to the Edge's CLI, and then run the required commands. See Secure Edge CLI Commands.

22.4 Secure Edge CLI Commands

Run the following CLI commands based on the configured access level.

Note: Run the help `command name` to view a brief description of the command.

Table 70: CLI Commands

Commands	Description	Access Level = Basic	Access Level = Privileged
Interaction Commands			
help	Displays a list of available commands.	Yes	Yes
pagination	Paginates the output.	Yes	Yes
clear	Clears the screen.	Yes	Yes
EOF	Exits the secure Edge CLI.	Yes	Yes
Debug Commands			
edgeinfo	Displays the Edge's hardware and firmware information. For a sample output of the command, see edgeinfo.	Yes	Yes
seainfo	Displays details about the Secure Edge Access of the user. For a sample output of the command, see seainfo.	Yes	Yes
ping, ping6	Pings a URL or an IP address.	Yes	Yes
tcpdump	Displays TCP/IP and other packets transmitted or received over the network attached to the Edge. For a sample output of the command, see tcpdump.	Yes	Yes
pcap	Captures packet data from network traffic and prints it to a file. For a sample output of the command, see pcap.	Yes	Yes
debug	Runs the debug commands for Edges. Run `debug-h` to view a list of available commands and options. For a sample output of one of the debug commands, see debug.	Yes	Yes
diag	Runs the remote diagnostics commands. Run `diag-h` to view a list of available commands and options. For a sample output of one of the diag commands, see diag.	Yes	Yes
ifstatus	Fetches the status of all interfaces. For a sample output of the command, see ifstatus.	Yes	Yes
getwanconfig	Fetches the configuration details of all WAN interfaces. Use the logical names such as "GE3" or "GE4" as arguments to fetch the configuration details of that interface. Do not use the physical names such as "ge3" or "ge4" of the WAN interfaces. For example, run `getwanconfig GE3` to view the configuration details of the GE3 WAN interface. Run the `ifstatus` command to know the interface name mappings. For a sample output of the command, see getwanconfig.	Yes	Yes

Commands	Description	Access Level = Basic	Access Level = Privileged
Configuration Command			
setwanconfig	Configures WAN interfaces (wired interfaces only). Run `setwanconfig-h` to view configuration options.	Yes	Yes
Edge Actions Commands			
deactivate	Deactivates the Edges and reapplies the initial default configuration.	No	Yes
restart	Restarts the SD-WAN service.	No	Yes
reboot	Reboots the Edge.	No	Yes
shutdown	Powers off the Edge.	No	Yes
hardreset	Deactivates the Edges, restores the Edge's default configuration, and restores original software version.	No	Yes
edged	Activates or deactivates the Edge processes.	No	Yes
restartdhcpserver	Restarts the DHCP server.	No	Yes
Linux Shell Command			
shell	Takes users into the Linux shell. Type exit to return to the secure Edge CLI.	No	Yes

To view sample outputs for various commands available within a secure Edge CLI, see Sample Outputs.

22.4.1 Sample Outputs

This section displays sample outputs for various commands available within a secure Edge CLI.

edgeinfo

```
o10test_velocloud_net:velocli> edgeinfo
Model:      vmware
Serial:     VMware-420efa0d2a6ccb35-9b9bee2f04f74b32
Build Version:  5.0.0
Build Date: 2021-12-07_20-17-40
Build rev:  R500-20211207-MN-8f5954619c
Build Hash: 8f5954619c643360455d8ada8e49def34faa688d
```

seainfo

```
o10test_velocloud_net:velocli> seainfo
{
  "rootlocked": false,
  "seauserinfo": {
    "o2super_velocloud_net": {
      "expiry": 1641600000000,
      "privilege": "BASIC"
    }
  }
}
```

tcpdump

```
o10test_velocloud_net:velocli> tcpdump -nnpi eth0 -c 10
reading from file -, link-type EN10MB (Ethernet)
09:45:12.297381 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 21
09:45:12.300520 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
09:45:12.399077 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 21
09:45:12.401382 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
09:45:12.442927 IP6 fd00:1:1:2::2.2426 > fd00:ff01:0:1::2.2426: UDP, length 83
09:45:12.444745 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 83
09:45:12.476765 IP6 fd00:ff01:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 64
09:45:12.515696 IP6 fd00:ff02:0:1::2.2426 > fd00:1:1:2::2.2426: UDP, length 21
```

pcap

```
o10test_velocloud_net:velocli> pcap -nnpi eth4 -c 10
The capture will be saved to file o10test_velocloud_net_2021-12-09_09-57-50.pcap
o10test_velocloud_net:velocli> tcpdump: listening on eth4, link-type EN10MB (Ethernet), capture
 size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

debug

```
o10test_velocloud_net:velocli> debug --dpdk_ports_dump
name         port  link  ignore  strip  speed  duplex  autoneg  driver
ge3             0     1       0      1   1000       1        1     igb
ge6             4     0       2      1      0       0        1   ixgbe
ge5             5     0       2      1      0       0        1   ixgbe
ge4             1     0       2      1      0       0        0     igb
sfp2            2     0       2      1      0       0        1   ixgbe
sfp1            3     0       2      1      0       0        1   ixgbe
net_vhost0      6     0       0      1  10000       1        0
net_vhost1      7     0       0      1  10000       1        0
```

diag

```
o10test_velocloud_net:velocli> diag ARP_DUMP --count 10
Stale Timeout: 2min | Dead Timeout: 25min | Cleanup Timeout: 240min
GE3
192.168.1.254        7c:12:61:70:2f:d0    ALIVE               1s

LAN-VLAN1
10.10.1.137          b2:84:f7:c1:d3:a5    ALIVE               34s
```

ifstatus

```
o10test:velocli> ifstatus
{
  "deviceBoardName": "EDGE620-CPU",
  "deviceInfo": [],
  "edgeActivated": true,
  "edgeSerial": "HRPGPK2",
  "edgeSoftware": {
    "buildNumber": "R500-20210821-DEV-301514018f\n",
    "version": "5.0.0\n"
  },
  "edgedDisabled": false,
  "interfaceStatus": {
    "GE1": {
      "autonegotiation": true,
      "duplex": "Unknown! (255)",
      "haActiveSerialNumber": "",
      "haEnabled": false,
      "haStandbySerialNumber": "",
      "ifindex": 4,
      "internet": false,
      "ip": "",
```

```
      "is_sfp": false,
      "isp": "",
      "linkDetected": false,
      "logical_id": "",
      "mac": "18:5a:58:1e:f9:22",
      "netmask": "",
      "physicalName": "ge1",
      "reachabilityIp": "8.8.8.8",
      "service": false,
      "speed": "Unkn",
      "state": "DEAD",
      "stats": {
        "bpsOfBestPathRx": 0,
        "bpsOfBestPathTx": 0
      },
      "type": "LAN"
    },
    "GE2": {
      "autonegotiation": true,
      "duplex": "Unknown! (255)",
      "haActiveSerialNumber": "",
      "haEnabled": false,
…
…
   }
  ]
}
```


getwanconfig


```
o10test_velocloud_net:velocli> getwanconfig GE3
{
  "details": {
    "autonegotiation": "on",
    "driver": "dpdk",
    "duplex": "",
    "gateway": "169.254.7.9",
    "ip": "169.254.7.10",
    "is_sfp": false,
    "linkDetected": true,
    "mac": "00:50:56:8e:46:de",
    "netmask": "255.255.255.248",
    "password": "",
    "proto": "static",
    "speed": "",
    "username": "",
    "v4Disable": false,
    "v6Disable": false,
    "v6Gateway": "fd00:1:1:1::1",
    "v6Ip": "fd00:1:1:1::2",
    "v6Prefixlen": 64,
    "v6Proto": "static",
    "vlanId": ""
  },
  "status": "OK"
}
```

Chapter 23

Configure User Account Details

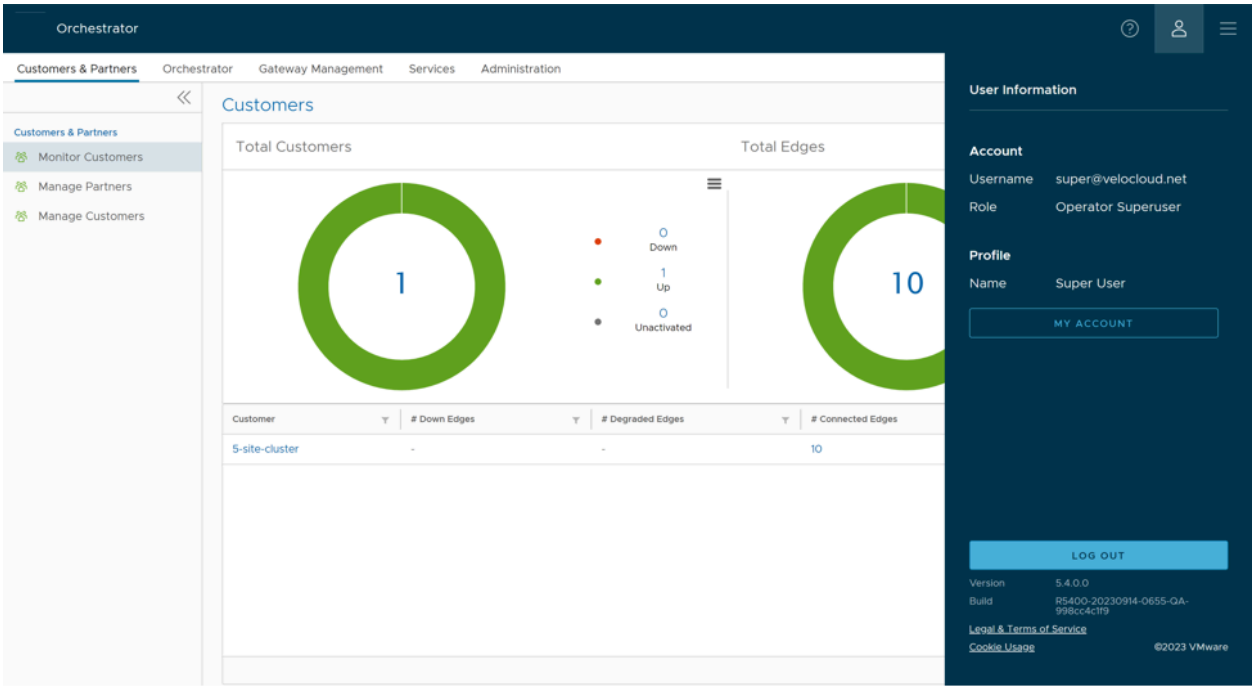
The **My Account** page allows users to configure basic user information, SSH keys, and API tokens. Users can also view the current user's role and the associated privileges.

Configure user privileges to securely access Edges. Choose the **Basic** access level for the user. Configure the access level when creating a new user (under User Management), and then modify it later. Only users with the Superuser role can modify a user's access level.

To access the **My Account** page, perform the following steps:

1. Select the **User** icon in the **Global Navigation** located at the top right of the screen.
   The **User Information** panel appears:

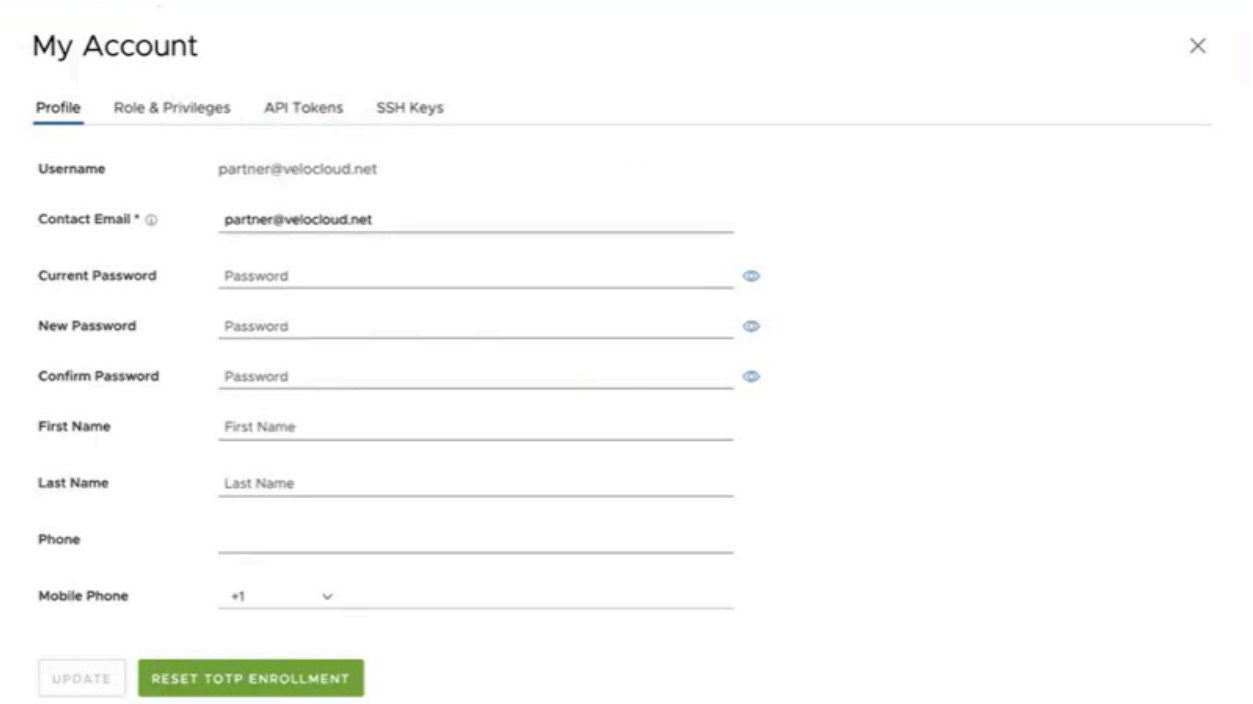
   Figure 23-1: User Information Panel



2. Select the **My Account** button.

The Orchestrator displays the **Profile** tab by default.

Figure 23-2: Configure My Account - Profile Details



3. Update the following basic user details:

Table 71: Profile tab - Options and Descriptions

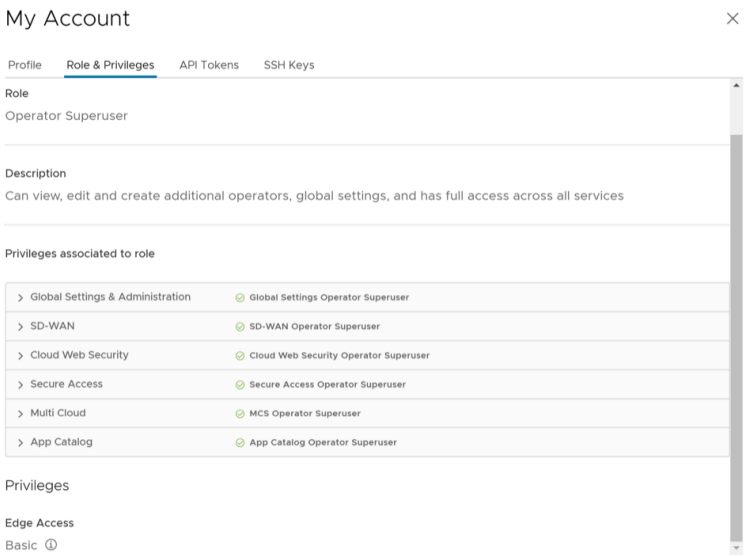
Option	Description
Username	Displays the username, and it is a read-only field.
Contact Email	Enter the primary contact email address of the user.
Current Password	Enter the current password.
New Password	Enter the new password. **Note:** The 4.5 release prohibits the special character '<' in passwords. Existing passwords containing the '<' character require an update before the system can save any changes.
Confirm Password	Re-enter the new password.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Phone	Enter the primary phone number of the user.
Mobile Phone	Enter the mobile number of the user along with the country code.

4. Select **Update** to save the user details.
5. Select **Reset TOTP Enrollment** to reset the existing enrollment.

Note: Changing the account password automatically resets the TOTP enrollment.

6. Select the **Role & Privileges** tab to view the existing user role and description. This tab also displays the privileges associated with the user role.

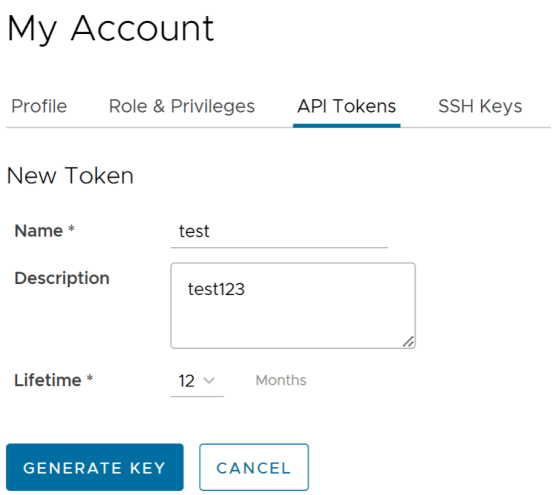
   Figure 23-3: Configure My Account - Role & Privileges Details



7. Select the **API Tokens** tab.

   The following screen is displayed.

   Figure 23-4: Configure My Account - API Tokens



8. Enter a **Name** and **Description** for the token, and then choose the **Lifetime** from the drop-down menu.
9. Select **Generate Key**.
10. Select the **SSH Keys** tab to configure a Secure Shell (SSH) key-based authentication.

    The SSH key-based authentication is a secure and robust authentication method to access VeloCloud Edges. It provides a strong, encrypted verification and communication process between users and Edges. The use of SSH keys bypasses the need to manually enter login credentials and automates the secure access to Edges.

Note:

- This feature requires Release 5.0.0 or later for both the Edge and the Orchestrator.
- Users with Operator Business or Business Specialist account roles cannot access Edges using key-based authentication.

For more information on SSH keys, see Add SSH Key.

11. After selecting the **SSH Keys** tab, select the **Generate Key** button. The following screen appears:

Figure 23-5: Configure My Account - SSH Keys

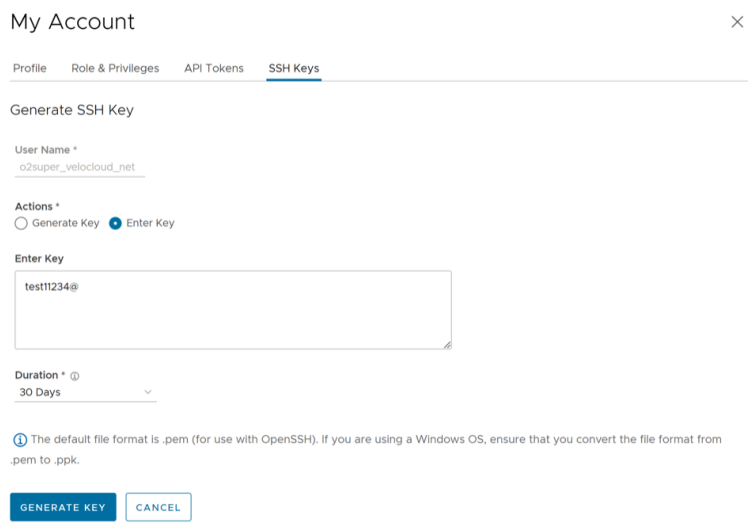


Table 72: SSH Keys - Options and Descriptions

Option	Description
User Name	Displays the username, and it is a read-only field.
Actions	Select either one of the following options: • **Generate key:** Use this option to generate a new pair of public and private SSH keys. **Note:** The system automatically downloads the generated key. SSH key generation uses the `.pem` format as the default. When using a Windows operating system, convert the file format from `.pem` to `.ppk`, and then import the key. For instructions to convert `.pem` to `.ppk`, see https://puttygen.com/convert-pem-to-ppk. • **Enter key:** Use this option to paste or enter the public key if users already have a pair of SSH keys.
PassPhrase	Choose to enter a unique passphrase to further safeguard the private key stored on the computer. **Note:** This is an optional field and is available only if a user has selected the **Generate Key** option.
Duration	Select the number of days by which the SSH key must expire.

12. Select **Generate Key**.

> **Note:** Each user account supports only one SSH Key.

13. To deactivate an SSH token, select the **Revoke** button. A pop-up window appears to confirm the revoke operation. Select the checkbox, and then select **Revoke** to revoke the key permanently.

    The system deletes the SSH keys for a user in the following cases:

    - Changing the user role to **Operator Business** or **Business Specialist** prevents Edge access via key-based authentication.
    - Deleting a user from the Orchestrator.

      > **Note:** Deleting or deactivating a user in an external SSO provider prevents them from accessing the Orchestrator. Only the explicit removal of the user from the Orchestrator deactivates the associated Secure Edge Access keys. Therefore, first delete the user from the IdP before deleting from the Orchestrator.

Enable Secure Edge Access for the Enterprise and switch the authentication mode from Password-based to Key-based. See Enable Secure Edge Access for an Enterprise Operator.

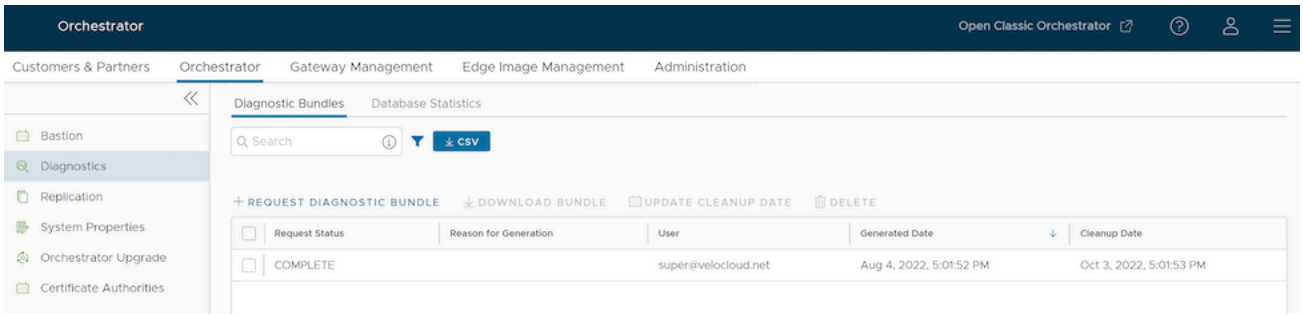
Chapter 24

Orchestrator Diagnostics

The Orchestrator Diagnostics bundle provides a collection of diagnostic information to troubleshoot the Orchestrator. For Orchestrator on premises installation, Operators can collect the Orchestrator Diagnostic bundle from the Orchestrator UI and provide it to the Arista Support team for offline analysis and troubleshooting.

In the Operator portal, navigate to **Orchestrator** > **System Properties**, and then set the System property `session.options.enableBastionOrchestrator` to **True** to view the **Diagnostics** tab.

Figure 24-1: Orchestrator Diagnostics



Use the following options to troubleshoot Orchestrator Diagnostics:

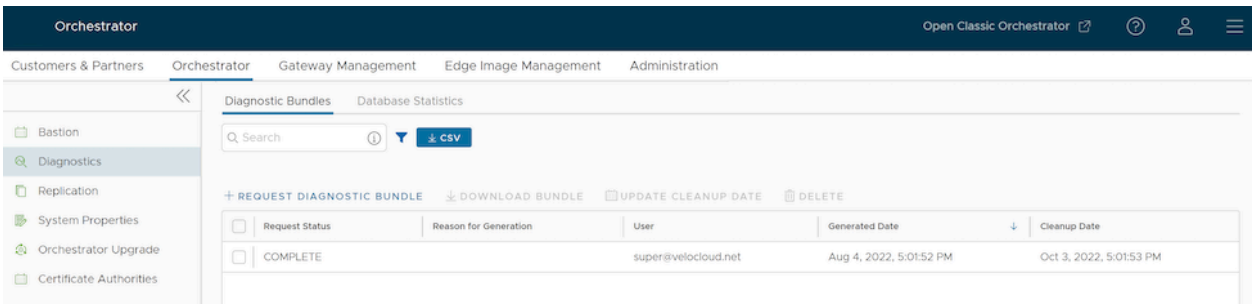
- **Diagnostic Bundles:** Request and download a diagnostic bundle.
- **Database Statistics:** Provides read-only access view for some of the information from a diagnostic bundle.

Diagnostic Bundles

To access the diagnostic bundles, perform the following steps:

1. In **Operator** portal, select **Orchestrator**.
2. Select **Diagnostics**. The **Diagnostic Bundles** page appears with the existing diagnostic bundles.

   Figure 24-2: Manage Diagnostic Bundles



   The **Orchestrator Diagnostics** table includes the following information:

Table 73: Orchestrator Diagnostics Field Descriptions

Field	Description
Request Status	The Request Status displays one of the following: • Complete • In Progress If a bundle has not completed the download, the **In Progress** status appears.
Reason for Generation	The specific reason for generating a diagnostic bundle. Select **Request Diagnostic Bundle** to include a description of the bundle.
User	The individual logged into the SD-WAN Orchestrator.
Generated	The date and time when the diagnostic bundle request sent.
Update Cleanup Date	The default **Cleanup Date** is three months after the generated date, and the bundle automatically deletes. If you wish to extend the cleanup date, select the **bundle**, then select this option to make the required changes. For additional information, see the **Update Cleanup Date** section below.

Requesting Diagnostic Bundle

To generate a new Diagnostic bundle perform the following steps:

1. Orchestrator Diagnostics **Request Diagnostic Bundle**.
2. In the **Request Diagnostic Bundle** dialog, enter the reason for generation.

Figure 24-3: Request Diagnostic Bundle

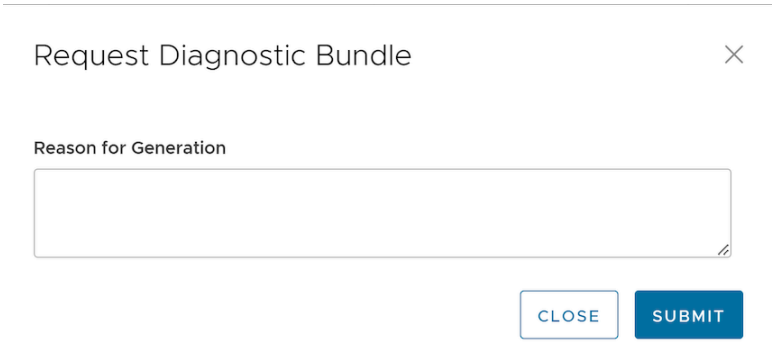


Table 74: Request Diagnostic Bundle Field Descriptions

Field	Description
Reason for Generation	Optionally, you can enter your reason for generating the bundle.

3. Select **Submit**.

The **Diagnostic Bundles** page displays the details of the generated bundleated, along with the status.

To search a specific diagnostic bundle, enter a relevant search text in the **Search** box. For advanced search, select the **Filter** icon next to the **Search** box to filter the results by specific criteria.

Downloade a Diagnostic Bundle

You can download the generated Diagnostic bundles to troubleshoot an Orchestrator.

To download a generated bundle, select the check box in the **Request Status** column and select **Download Bundle**. The bundle downloads as a ZIP file.

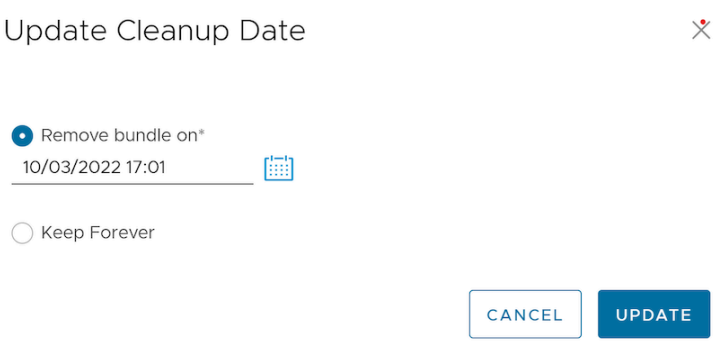
You can send the downloaded bundle to the Arista Support representative for debugging the data.

Update Cleanup Date

The completed bundles automatically delete on the date displayed in the **Cleanup Date** column.

1. To update the cleanup date of a generated bundle, select the check box in the **Request Status** column and select **Update Cleanup Date**.
2. In **Update Cleanup Date** , choose the date for the selected bundles to delete and select **Update**.

   Figure 24-4: Update Cleanup Date



3. Select **Keep Forever** to retain the bundle, so that the bundle does not delete automatically.
   The Orchestrator Diagnostics table updates to reflect the changes to the Cleanup Date.

Deleting a Diagnostic Bundle

To delete a bundle manually, select the check box in the **Request Status** column and select **Delete**.

Database Statistics

The **Database Statistics** tab provides read-only access view of the information from a diagnostic bundle. To view it, select **Database Statistics**.

If you require additional information, go to **Diagnostic Bundles**, to request a diagnostic bundle and download it locally.

The **Database Statistics** tab displays the following information:

Figure 24-5: View Database Statistics - Example 1

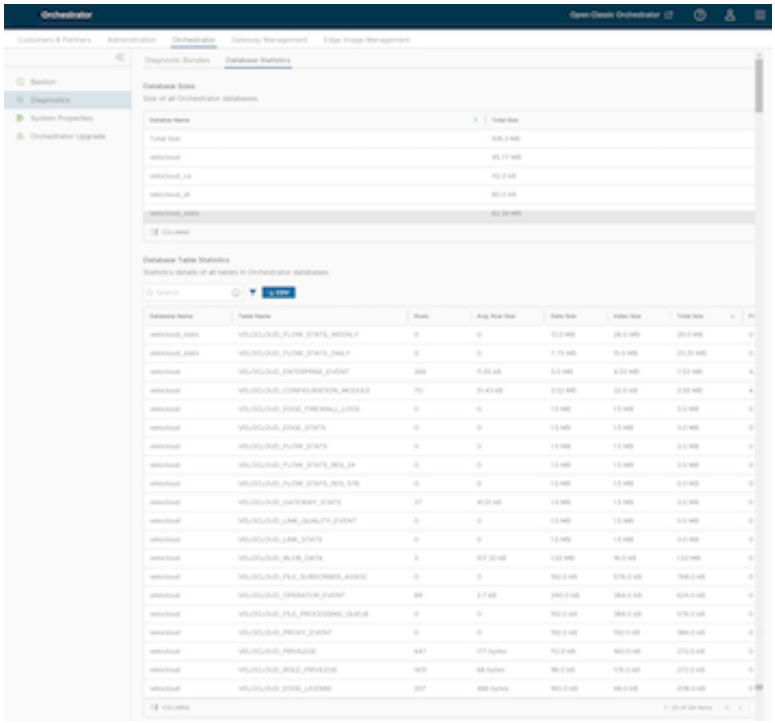


Figure 24-6: View Database Statistics - Example 2

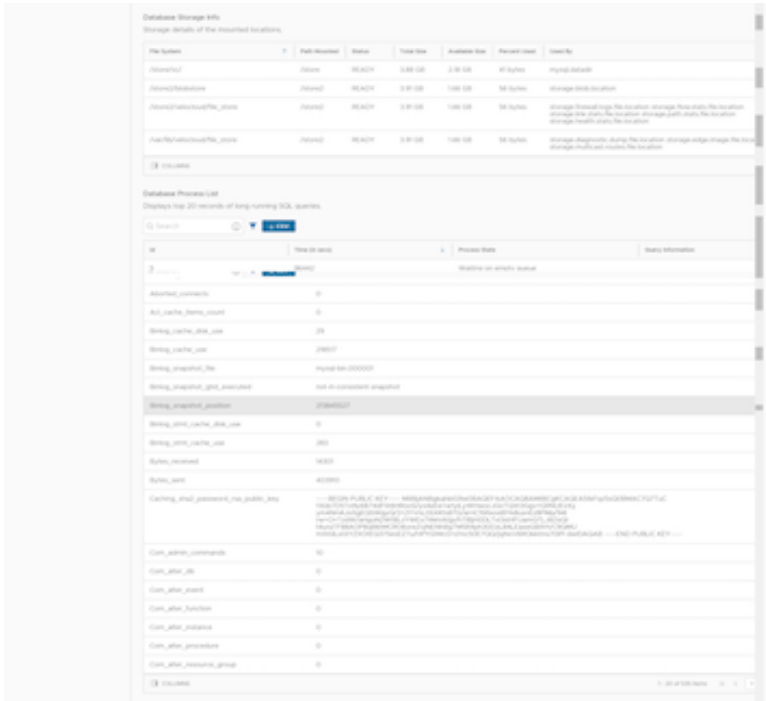


Figure 24-7: View Database Statistics - Example 3

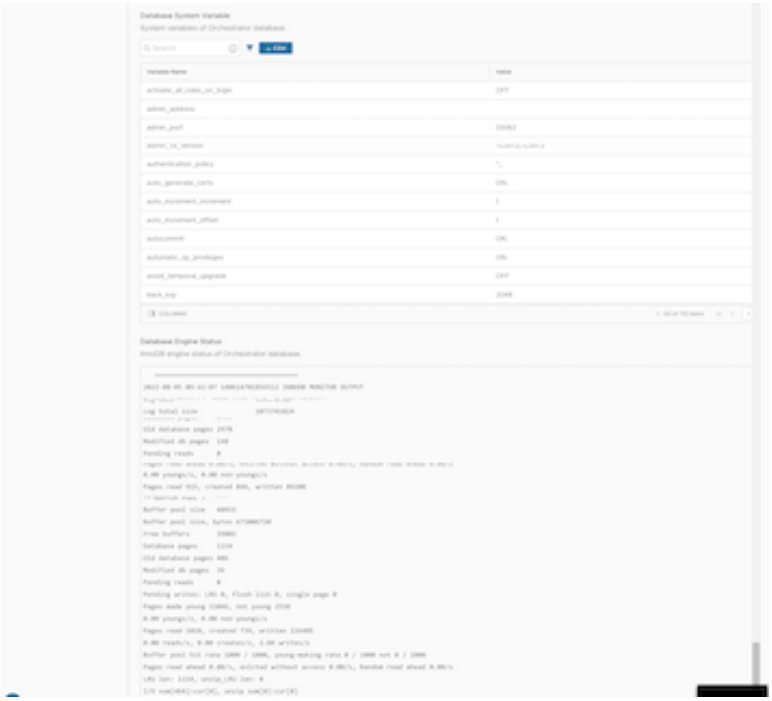


Table 75: Database Statistics

Field	Description
Database Sizes	Sizes of the Orchestrator databases.
Database Table Statistics	Statistical details of all tables in the Orchestrator database.
Database Storage Info	Storage details of the mounted locations.
Database Process List	The top 20 records of long-running SQL queries.
Database Status Variable	The status variables of the MySQL server
Database System Variable	System variables of the MySQL server.
Database Engine Status	The InnoDB engine status of the MySQL server.

Chapter 25

Orchestrator Upgrade

This section discusses the prerequisites and steps required to upgrade a Orchestrator. Orchestrator allows you to configure and send a banner message about an upcoming Orchestrator upgrade. The banner displays to users after the next log into the Orchestrator. You can customize the banner message and visibility for the users.

To upgrade a Orchestrator, perform the following steps:

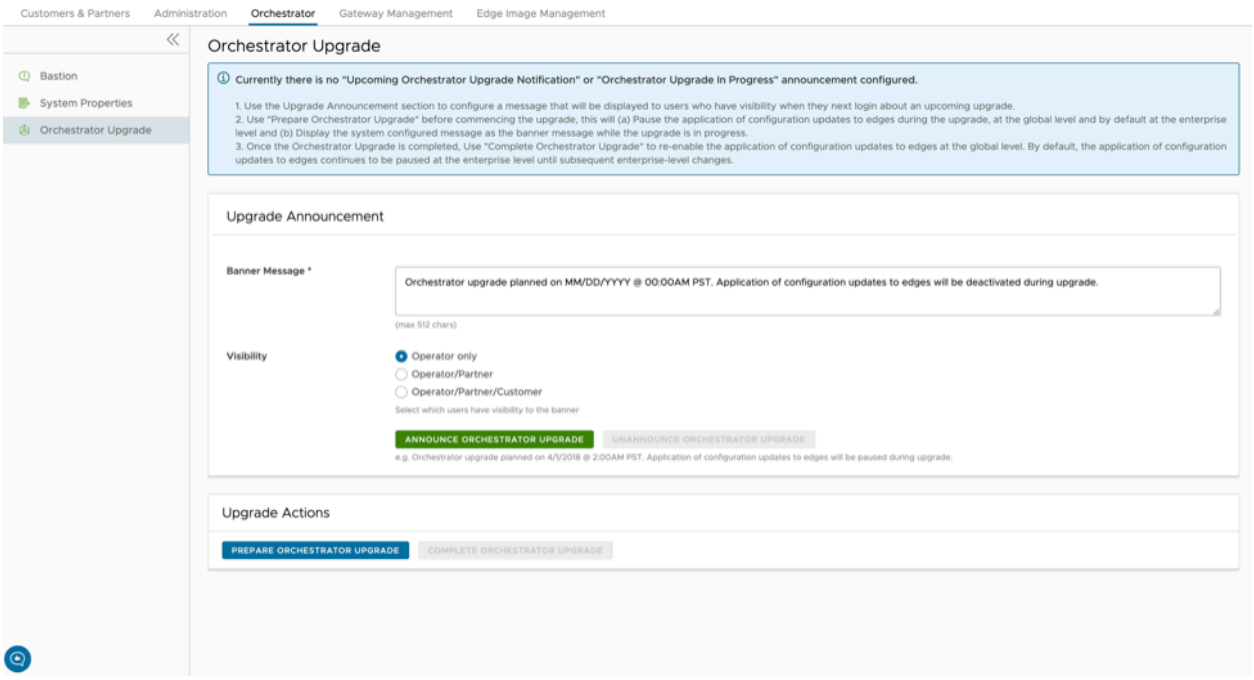
1. Configure Orchestrator Upgrade Announcement.
2. Prepare Orchestrator Upgrade.
3. Complete Orchestrator Upgrade.

Configure the Orchestrator Upgrade Announcement

The **Upgrade Announcement** area enables you to configure and send a message about an upcoming upgrade. To send an Orchestrator Upgrade announcement, perform the following steps:

1. In the **Operator** portal, select **Orchestrator**, and go to **Orchestrator Upgrade**. The **Orchestrator Upgrade** screen displays.

   Figure 25-1: Orchestrator Upgrade Screen



2. Under **Upgrade Announcement**, set the banner message and visibility for the users.

Table 76: Upgrade Announcement Option Descriptions

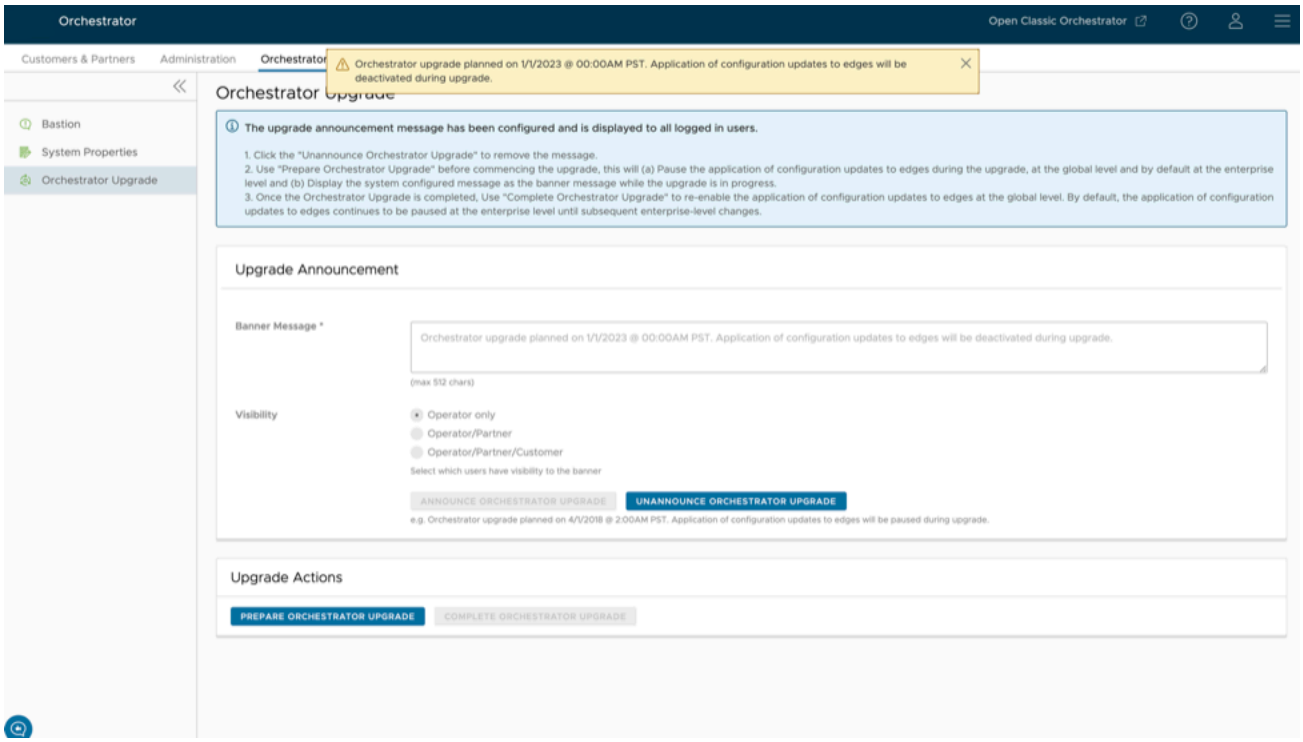
Option	Description
Banner Message	Enter the required **Banner Message** in the textbox to announce the status of an upcoming upgrade. A messages displays indicating successful creation of your announcement, and your banner message displays at the top of the Orchestrator.
Visibility	You can choose the banner **Visibility** for the users. By default, **Operator only** is selected.

3. Select **Announce Orchestrator Upgrade** to display the banner message. A message displays indicating that you have successfully created your announcement, and that your banner message displays at the top of the Orchestrator.
4. If you want to remove the announcement from the Orchestrator, select **Unannounced Orchestrator Upgrade**. A message displays indicating that you successfully unannounced the Orchestrator upgrade.

Prepare the Orchestrator Upgrade

After you have configured the Orchestrator upgrade banner message and visibility for the users, select **Prepare Orchestrator Upgrade**. This pauses the application of the configuration updates of Edges during the upgrade, at the global level and by default, at the enterprise level. It displays the system configured message as the banner message while the upgrade progress.

Figure 25-2: Orchestrator Upgrade Message



Contact the Arista Support team to prepare for the Orchestrator upgrade.

1. Collect the following information prior to contacting Support:
   - Provide the current and target Orchestrator versions, for example, current version and target version.

> **Note:** For the current version, this information can be found by selecting the **Help** icon.

- Provide a screenshot of the replication dashboard of the Orchestrator.
- Hypervisor Type and version Commands from the Orchestrator:

> **Note:** Commands must be run as root (e.g. '**sudo <command>**' or '**sudo -i**').

  - Run the script `/opt/vc/scripts/vco_upgrade_check.sh` to check:
    - LVM layout
    - Memory Information
    - CPU Information
    - Kernel Parameters
    - Some system properties
    - ssh configurations
    - MySQL schema and database sizes
    - File_store locations and sizes
  - Copy of `/var/log`

```
tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log
```

  - From the Standby Orchestrator:

```
sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS
 \G'
```

  - From the Active Orchestrator:

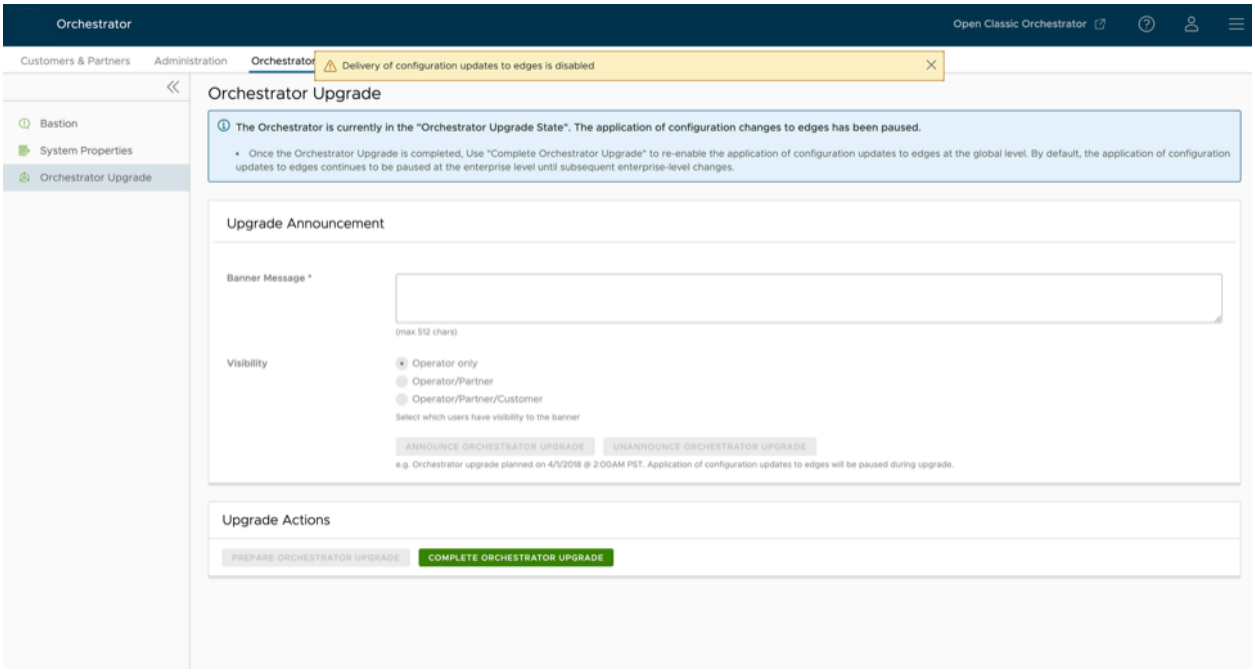
```
sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER
 STATUS \G'
```

2. Contact Arista Support with the information for assistance with the Orchestrator upgrade.

Complete the Orchestrator Upgrade

After you complete the Orchestrator upgrade, select **Complete Orchestrator Upgrade** under **Upgrade Actions**. This re-enables the application of the configuration updates of Edges at the global level.

Figure 25-3: Orchestrator Upgrade Actions



To verify that the status of the upgrade as complete, run the following command to display the correct version number for all the packages:

```
dpkg -l|grep vco
```

When you are logged in as an Operator, you can confirm if the same version displays by selecting the **Help** icon at the top right corner of the page.

Chapter 26

Replication

Information regarding how to set up Arista Edge Cloud Orchestrator Replication, also known as Disaster Recovery (DR), is available in the section *Configure Arista Edge Cloud Orchestrator Disaster Recovery* of the *Arista Cloud Orchestrator Deployment and Monitoring Guide*.

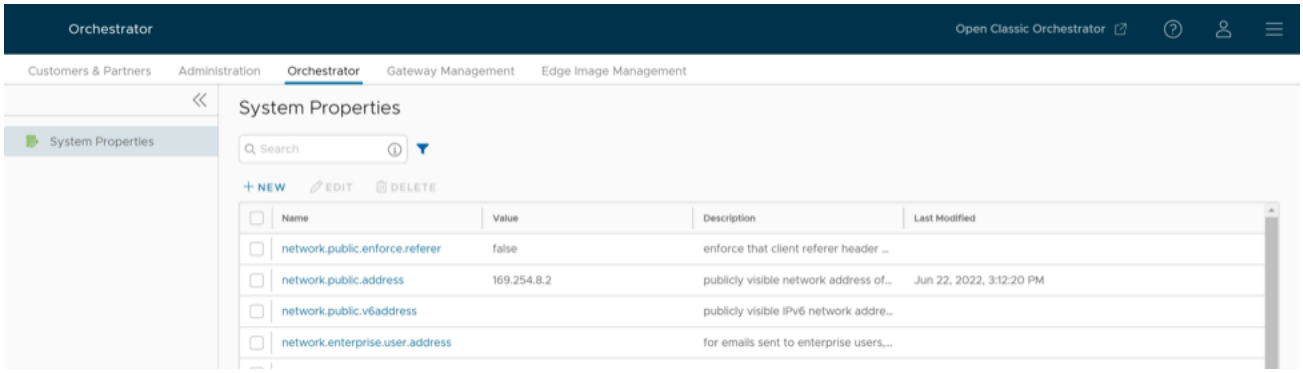
Chapter 27

System Properties

Arista provides System Properties to configure various features and options available in the Orchestrator portal.

In the Operator portal, navigate to the **System Properties** page, which lists the available pre-defined system properties. You can modify some of the system properties as an Operator.

Figure 27-1: Manage System Properties



To configure the system properties:

1. Select **New System Property** to add a new property.

2. In the **New System Property** window, configure the following parameters:

Figure 27-2: Create New System Property

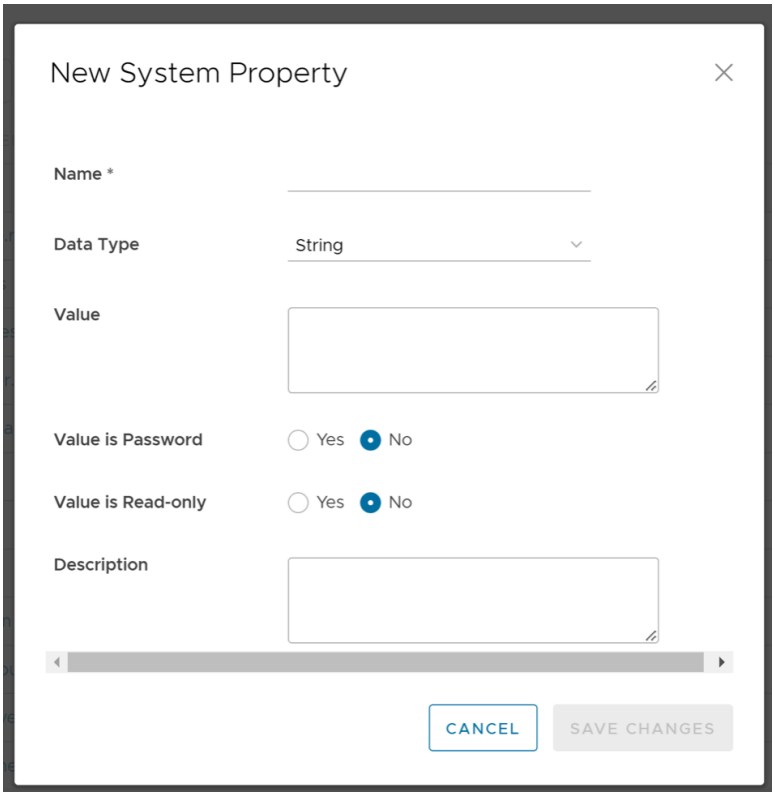


Table 77: New System Property Option Descriptions

Option	Description
Name	Enter the **Name** for the new system property.
Data Type	Choose the required **Data Type** from the drop-down menu.
Value	Enter the **Value** for the property according to the data type.
Value is Password	Select **Yes** or **No** as required.
Value is Read-only	Select **Yes** or **No** as required.
Description	Enter the **Description** for the new system property.

3. Select **Save Changes**

   a. You can use the **Search** field to find a specific system property.

   See the section, *List of System Properties* in the *Arista VeloCloud Orchestrator Deployment and Monitoring Guide*, which lists the system properties that you can modify as an Operator.

> **Note:** Contact Arista Support before making any changes to the system properties as recommended.

Chapter 28

External Certificate Authority

The External Certificate Authority (CA) feature is for large enterprises and government customers who deploy an on-premise Orchestrator and have a requirement to use their own certificate authority (CA) rather than the default self-signed Orchestrator certificate authority. This section covers how to enable and configure the External CA.

hen you configure an External CA, instead of the Orchestrator receiving a certificate signing request (CSR) and issuing device certificates itself, the Orchestrator must pass the CSR to the external CA for issuance. The device certificate will be returned to the Orchestrator and sent to the Edge or Gateway.

The system expects that when a customer uses this feature to deploy a commercial certificate authority, for example, PrimeKey (EJBCA PKI), or, in some cases, to have implemented their own proprietary CA.

Beginning with Release 5.1.0, an Orchestrator where external CA is activated may be configured with two new API-ready modes:

- **Manual Mode** supports any certificate authority and offers flexibility and control, with the user manually performing each step in the certificate process.
- **Asynchronous Mode** supports any certificate authority, enabling scriptable manual steps and automated recurring tasks.

The very first mode, **Synchronous or Automated Mode**, includes these modes. In Synchronous mode, the Orchestrator integrates directly with an external CA (which, for Release 5.0.0 and later, offered PrimeKey EJBCA PKI as the only available external certificate authority) and via REST APIs for certificate requests, renewals, and revocations.

Enable External CA

The Operator Superuser must enable the External CA feature through two specific System Properties. Only an Operator with the Superuser role can modify these settings.

Procedure

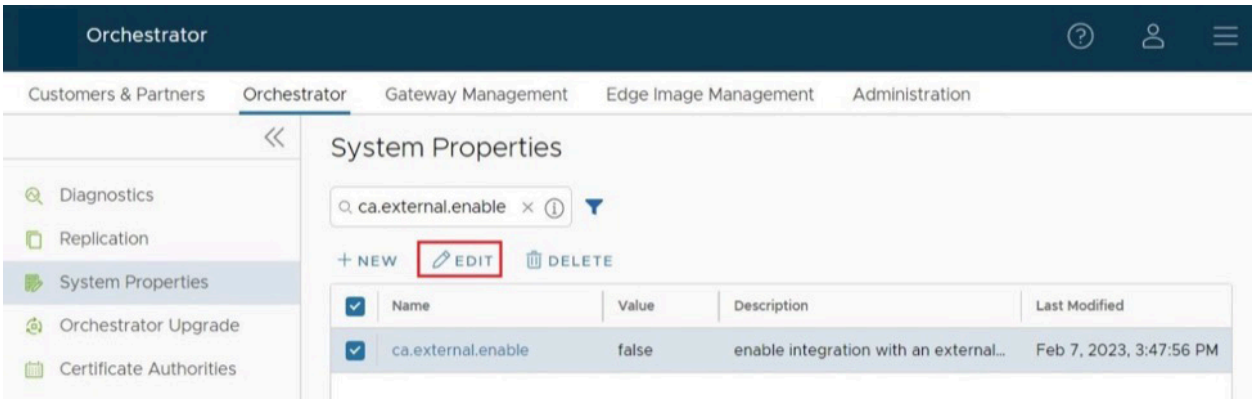
Enable the `ca.external.configuration` first. The system creates this property manually with a JSON data type, and the JSON is populated consistently with the example shown in the Sample External CA Configuration section.

Only after the `ca.external.configuration` is created and enabled, should the Operator enable the second system property: `ca.external.enable`.

1. On the Orchestrator UI, select **System Properties**.

2. Using the search box on the **System Properties** page, enter `ca.external.enable` as shown in the following image.

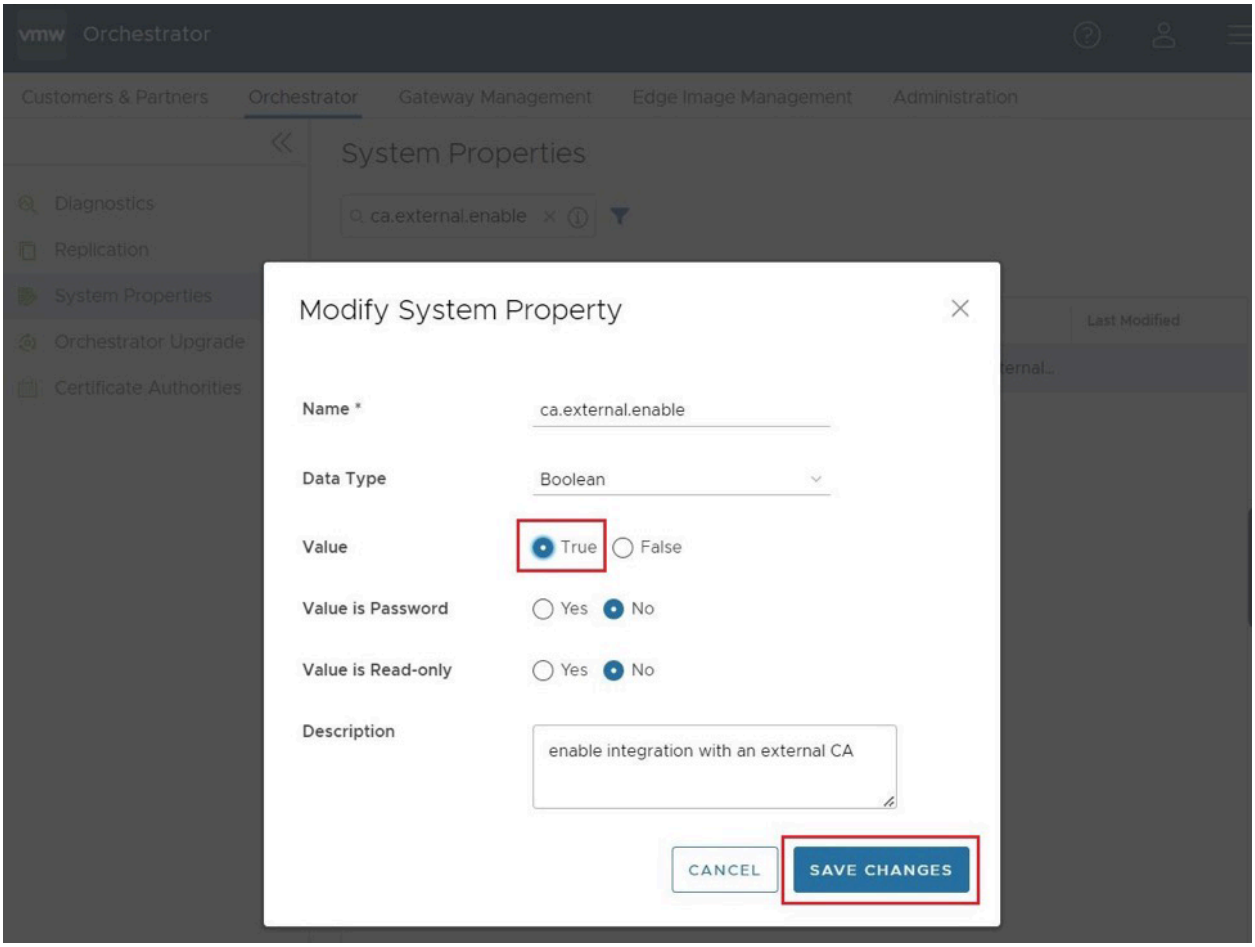
Figure 28-1: Edit System Properties



3. After the `ca.external.enable` property is located, either select that property or check the box and select **Edit**.

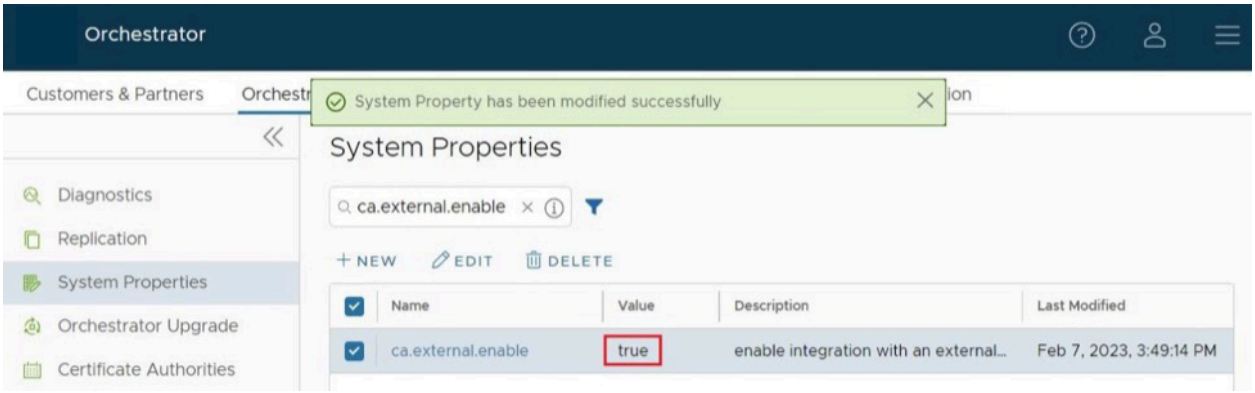
4. Set the `ca.external.enable` property to **True**, then select **Save Changes** to complete the change, as shown in the following image.

Figure 28-2: Modify System Properties



The **System Property** page displays a confirmation that the property was successfully modified, that `ca.external.enable` is now **True**.

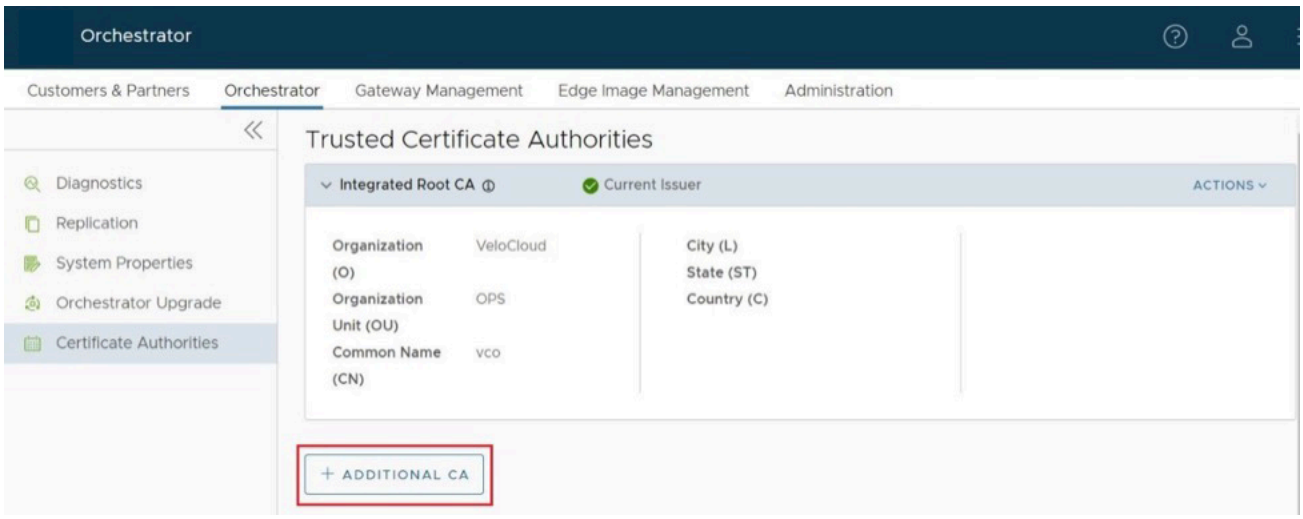
Figure 28-3: Confirm System Properties



Configure External CA

After enabling the External CA System Property, the Operator can now select **Orchestrator** > **Certificate Authorities** to begin configuring an external certificate authority.

Figure 28-4: Configure Certificate Authorities

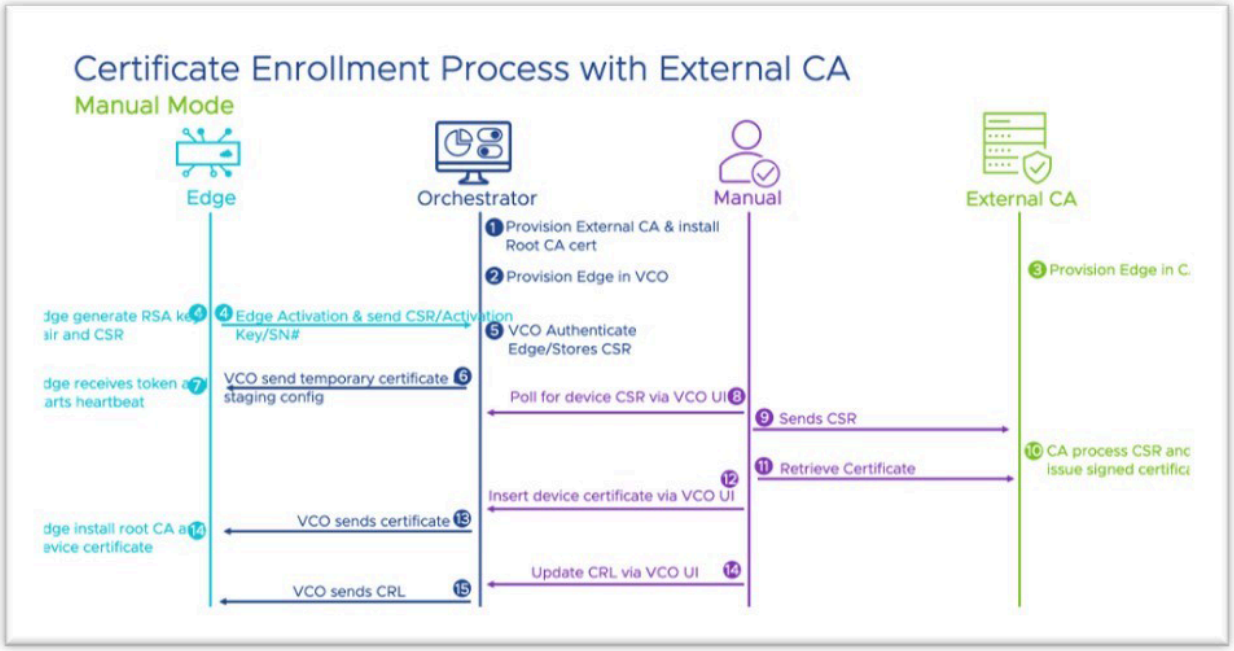


Configuring an External CA can be done using one of three modes:

1. **Automated (Synchronous):** With **Automated** mode, only one external certificate authority is supported: **PrimeKey EJBCA PKI**.

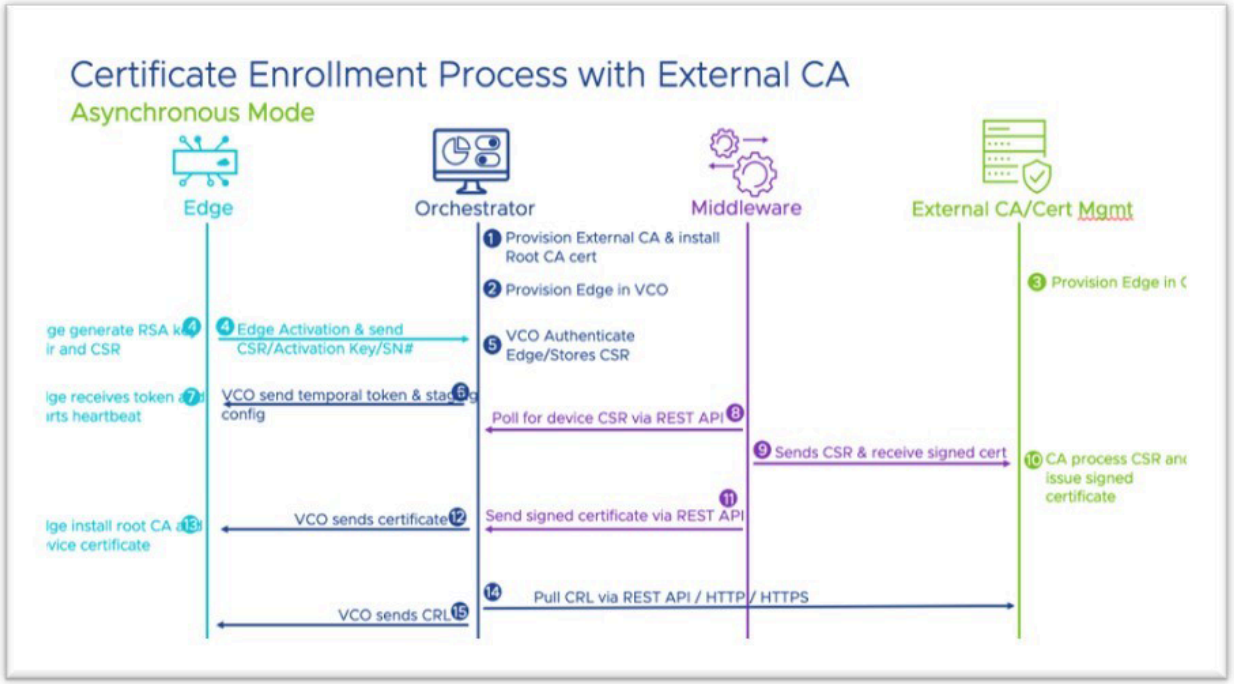
2. **Manual:** Manual mode supports any certificate authority and offers flexibility and control, with the user performing each step in the certificate process.

Figure 28-5: Manual Mode for Certificate Processing



3. **Asynchronous:** Asynchronous Mode supports any certificate authority and allows scripting manual steps while automating recurring tasks.

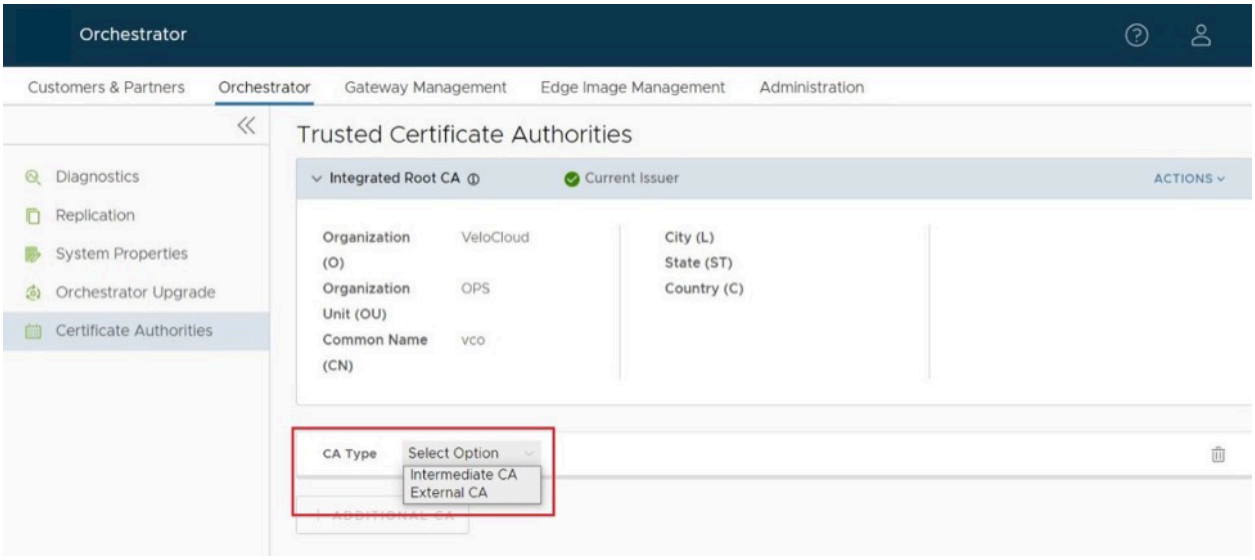
Figure 28-6: Asynchronous Mode for Certificate Processing



1. On the **Orchestrator** > **Certificate Authorities** page, select **+ Additional CA**.

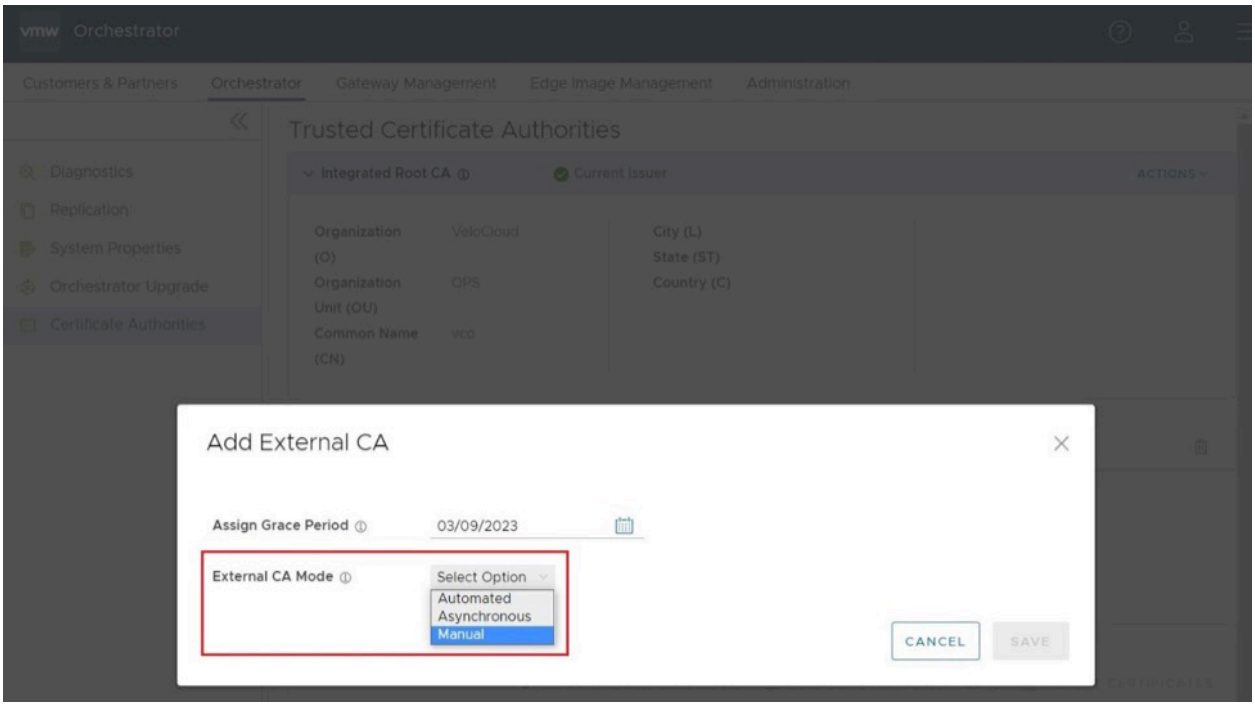
2. After selecting **+ Additional CA**, the UI will change to **CA Type** with a drop-down menu offering **Intermediate CA** and **External CA**. Select **External CA**.

   Figure 28-7: Add Additional CA



3. After the External CA is selected, the screen changes to the **Add External CA** screen where an Operator can choose between the three previously mentioned External CA Modes: Automated (Synchronous), Asynchronous, and Manual.

   Figure 28-8: Select CA Modes



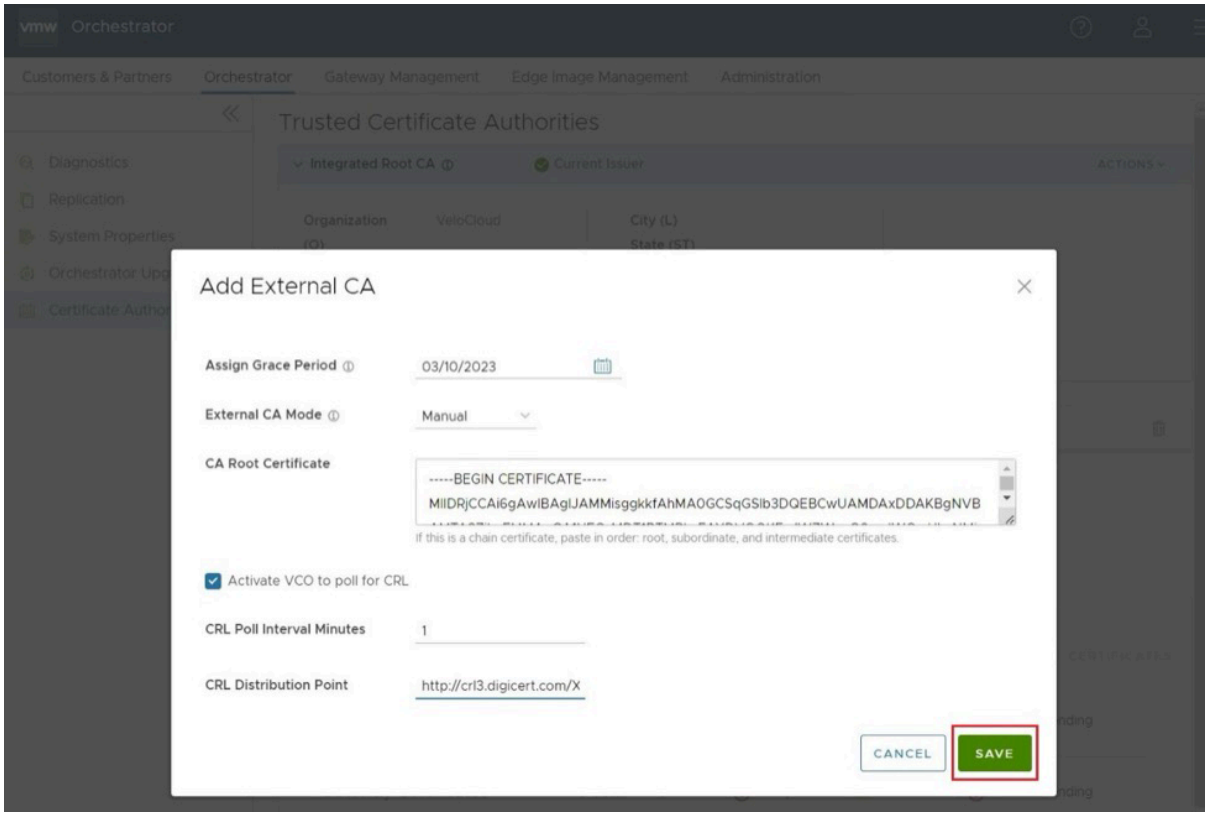
4. After selecting a CA Mode, the **Add External CA** screen changes to allow further configuration of the external CA. Here, the Operator would paste in the **CA Root Certificate**.

   By checking the **Activate VCO to poll for CRL** box , the Operator elects to have the Orchestrator to conduct certificate revocation checks using the Certificate Revocation List (CRL). When you select this option, two additional configuration parameters appear to be configured by the Operator:

   a. **CRL Poll Interval in Minutes** determines how often in minutes the Orchestrator will check the latest CRL for certificate revocation.

   b. **CRL Distribution Point** is the URL where the Orchestrator retrieves the latest CRL.

   Figure 28-9: Latest CRL Distribution Point



5. After the Operator fills the required fields, they would select **Save**.

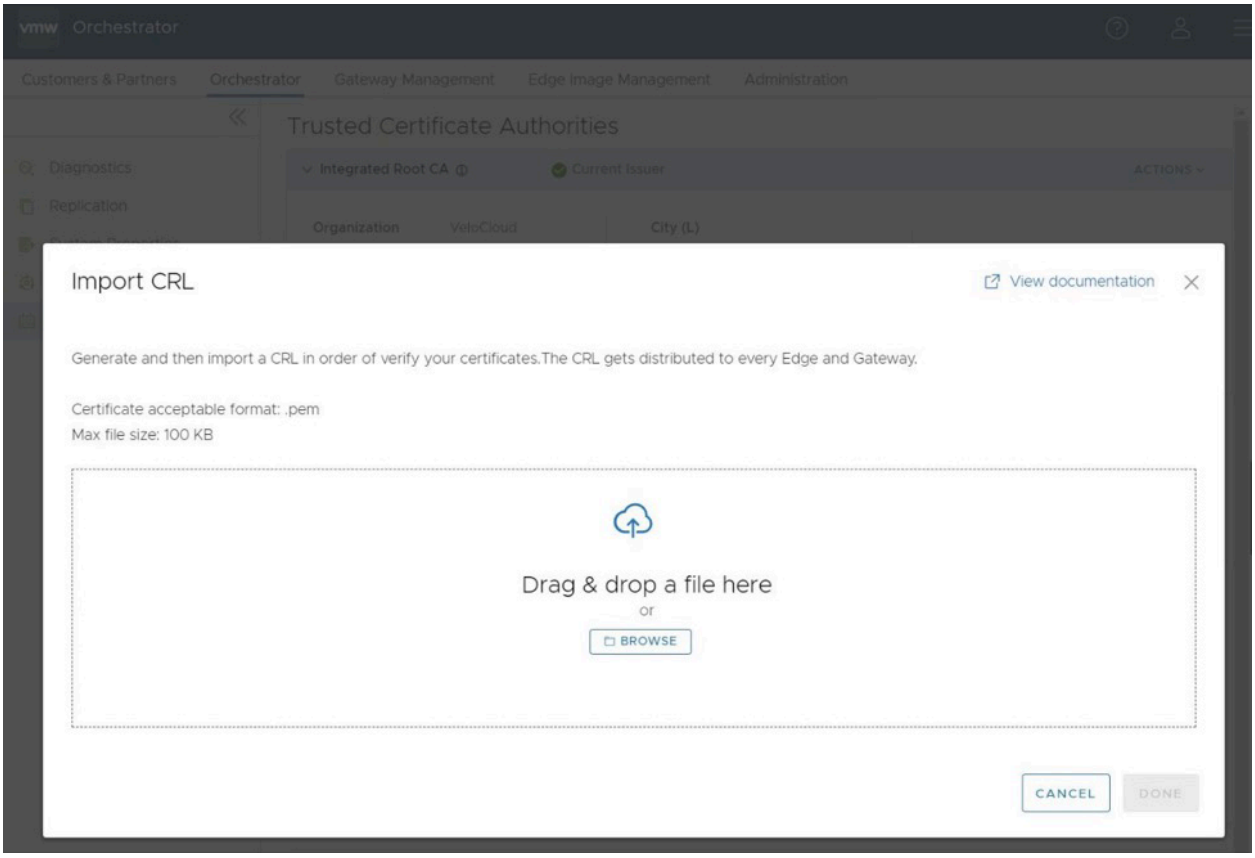
6. After configuring an external CA, the Operator will have newly available options to **import CRL** and **download CRL**.

Figure 28-10: Import CRL

Figure 28-11: Download CRL

Using **Import CRL** while also having **Orchestrator CRL Polling** configured, an Operator can perform batch or individual imports and exports.

Figure 28-12: Batch Import and Exports



The CRL would perform a validation after any import of your certificates, and the Orchestrator distributes your CRL to every Edge and Gateway connected to your Orchestrator.

Note: There is a third System Property: `ca.external.caCertificate`. This System Property appears after enabling External CA, and it establishes connectivity to a valid external CA. This property requires a PEM (Privacy-Enhanced Mail)- encoded certificate.

Note: An Edge/Gateway-generated Certificate Sign Request (CSR) contains only a Common Name (CN). While signing the CSR, the External CA adds the required subject.

Sample External CA Configuration

This section provides an example of a configuration for the `ca.external.configuration` field.

```
{
  "integrationType": "SYNCHRONOUS",
  "csrDistinguishedName": {
    "CN_PID_SN": "VMWare-SDWAN"
  },
  "synchronous": {
    "synchronousIntegrationType": "EJBCA",
    "ejbca": {
```

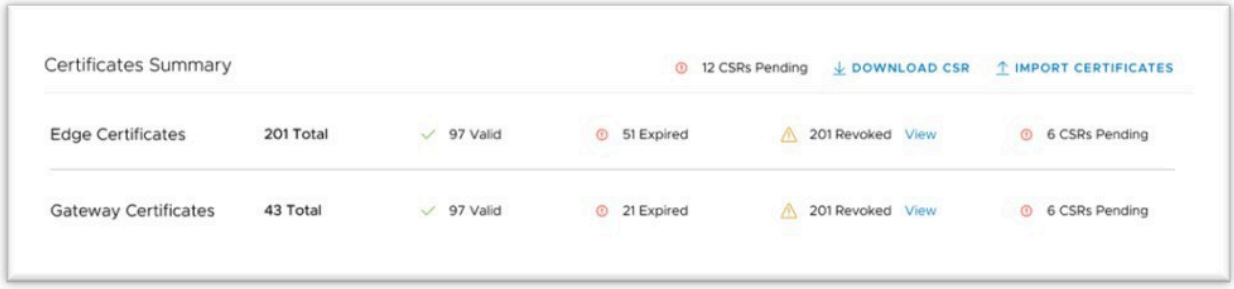
```
      "serverCaCertificate": "-----BEGIN CERTIFICATE-----\nMIIFFzCCA3+gAwIBAgIUGgattlewRnm/gy
PxJ7PW6uJOjCcwDQYJKoZIhvcNAQEL\nBQAwgZIxIzAhBgoJkiaJk/IsZAEBDBNyLTA1OTVhMTNjMTUzZDc2YWU1MRU
wEwYD\nVQQDDAxNYW5hZ2VtZW50Q0ExHjAcBgNVBAsMFWFtaS0wMmE0NDc0YzFmNzQ5NDBh\nODE0MDIGA1UECgwraX
AtMTAtODEtMTI1LTEzMi51cy13ZXN0LTIuY29tcHV0ZS5p\nbnRlcm5hbDAeFw0yMTAyMDQxOTA0MTRaFw00NjAyMDU
xOTA0MTNaMIGSMSMwIQYK\nCZImiZPyLGQBAQwTci0wNTk1YTEzYzE1M2Q3NmFlNTEVMBMGA1UEAwwMTWFuYWdl\nbW
VudENBMR4wHAYDVQQLDBVhbWktMDJhNDQ3NGMxZjc0OTQwYTgxNDAyBgNVBAoM\nK2lwLTEwLTgxLTEyNS0xMzIudXM
td2VzdC0yLmNvbXB1dGUuaW50ZXJuYWwwggGi\nMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQC2r0YYVKnusA7N
S6aCSjbRdzMA\nNgbF1j3+aeWn6ZokjpFsk9Tavnu0c9gETIMfVVFj6jCyTLZcHWuPt2r1aEfvuDyk\nW/u4kY8IaGS
E5Z5+QH2I8gifTfegQBqFBSk8q4dN7oOnoXFKhUgCRtTf6hd7aSji\nynnIUkEV6P/t5q+Mwql1EK6RdZzL6w9ycQOkG
7mitfW4onJJcbIKy3abB/vkiTmd8\nSQ10DyDXOzN6gwCrcUV0RfxIgd4YKN8Cj+/+bMw+It8mn5Dd/xl9FutYAQ+br
Zhy\nSDw5m2W66y/znh3Fr1+DUn8b0wlgHrwPSi9i/QlOefRDMvFmjiDyXq+E/peirDyl\njVxYwn0ySgO5TympwkWw
1Riibp4fJpYtwYT4EJU85em1rD6PPrzfBPsGQeG4ljQE\nCZ2YrnOLctbv+sF5rYQzTl0lOrLMAuqJLyV4Shv+3Oj1S
zXKwkqJC0sCLcX+djmq\nYOJ9YxBke7DQKubTezHkyuk9tarEq5iHr68Ig3sCAwEAAaNjMGEwDwYDVR0TAQH/\nBAUw
AwEB/zAfBgNVHSMEGDAWgBRp8EFk1aYW+s/tweOUwuXh/xuMJzAdBgNVHQ4E\nFgQUafBBZNWmFvrP7cHjlMLl4f8bj
CcwDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3\nDQEBCwUAA4IBgQCzAO0RZIHJUJw2xbcLr2Cvr0tj+3qbY5f/LYN5Gf
yMk5RjLK+u\nbaius7FxpRpw40oZ/FH2ichDD4FO8ulqJt4znU3VtwJ0/JmaY2x0XqwEI0CWiEiE\naKiSMzaHjsMvJ
7gNQSfcB+QEm8IM/PSPKcxNj2+QnHtDnQwgb5iMN6n88Bjeygrk\nJG0RH0EUJ0sQr9pXo+Gcn66b99HgEyIjojqsGC
1dYzkZVHQuFH7RINfU//1OmnRN\nmb6JgjNGgbdPKKHdWrfwrGpCiz1c44yznlkWVFrMdbLA1B+1uLpb8Xka7Hq5qZZ
n\nLVC0O7Q483FBa8Lkg+RXQjIxYXgx4wkiV600UyKP1pwNSLMJvUUBmIM/Byl1h8xR\nyKIIZn7rc5wA4aKcfnJ9CU
VfKCjtUPZffOWlvMt8bDZfaloif20Z0KydJyAStl3Z\nQbsMvcA6747aQQ25JD4tid5rDeRDb2bYi7nLl+lNnhmn5ZB
4qGgnaXGj3oFDoN0R\n+kEK69DlZRNudn4=\n-----END CERTIFICATE-----",
      "apiCertificate": "-----BEGIN CERTIFICATE-----\nMIIEKzCCApOgAwIBAgIUM83EYfZz4vi4ty
1EOJr+n6wMksAwDQYJKoZIhvcNAQEL\nBQAwgZIxIzAhBgoJkiaJk/IsZAEBDBNyLTA1OTVhMTNjMTUzZDc2YWU1MRU
wEwYD\nVQQDDAxNYW5hZ2VtZW50Q0ExHjAcBgNVBAsMFWFtaS0wMmE0NDc0YzFmNzQ5NDBh\nODE0MDIGA1UECgwraX
AtMTAtODEtMTI1LTEzMi51cy13ZXN0LTIuY29tcHV0ZS5p\nbnRlcm5hbDAeFw0yMTAyMDUwMDA1MTRaFw0yNjAyMDU
wMDA1MTNaMBUxEzARBgNV\nBAMMClN1cGVyQWRtaW4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC/\nrP
dG0oY89GGUgHbV9iG3n3Y1mPBmQ+iVBvKYD3YpM7fG+KnVQTdJLrYoH5vP7lVY\nQj9H6pjxq0Bh53Mse2Fl9UE/Gew
6IZiRd2OK9yM1xRKH7hjPB3tqFlA98mar+BYA\nGPhapmq+sSFz6TS2ssToUllG8QgJeMxh6+vSP/Ca9O+HiDB7TqEC
ufVv6lrL7sfK\nqfyQ5YzITKm7IGDQfdCiorwndvd1i1NB+vviiYsk1fEW8gvRUu7wMRlzmPwxnUxd\nKmb/b7+O65m
d7+FlkqU6EzYMQ/224ZJonwJfzmNTO1AGt4aaJDNKn1i5wV22xqqQ\nZvA6nrkBd+06pUwVTen1AgMBAAGjdTBzMAwG
A1UdEwEB/wQCMAAwHwYDVR0jBBgw\nFoAUafBBZNWmFvrP7cHjlMLl4f8bjCcwEwYDVR0lBAwwCgYIKwYBBQUHAwIwH
QYD\nVR0OBBYEFFj+bk/epA/jPXZywy1D4XV5sWlMMA4GA1UdDwEB/wQEAwIF4DANBgkq\nhkiG9w0BAQsFAAOCAYEA
RNN08PUMCAWI+wLpu4FRuApRJrWn7U07D2ZDirV5a7pq\nICCbREe34EYmbLyqdUCMHS8xJlPun5ER3E5YFzckC7wJ9
y2h8giB7O3cjx/wWkax\nNEkz/Is634XZveIRNf1TmV9/71LnfUBDJjHYFPNzyw6CBtVn/niL1Q9o3SvbbZLQ\nCcdc
pFm1rxku0UOuCaQgOSuLn5nqTFCNi4Sx40shg8wDrc1AUuv+yX09dM2G+27h\ndCJrkqHwbtWQMY2sOBdTIq6TMyJyr
svTCTQ67vqRtdJuSqOw/CnPnSo2/lSrkNWC\nIl7mQzq6+2ayQBxsm6xuHXD0INoRB+flq/QhY+CQIaTLYLezVITo0b
Zhe0TpNqYK\nlINUWjxI8mCBBiXZZ9zxbyOqzZouZcNH12OCEqU8alTfyW0EpGYClemRTgXxboDK\n+uEwKH6sngYMk
G0Usni4WIKBvZV2dJa5o8RhuCUFhwBJ2aHuiTq86RLrazJBE3wA\nGvpl0ZmGVYmond3aBOYu\n-----END CERTIFICATE--
---",
      "apiKey": "-----BEGIN PRIVATE KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/
rPdG0oY89GGU\ngHbV9iG3n3Y1mPBmQ+iVBvKYD3YpM7fG+KnVQTdJLrYoH5vP7lVYQj9H6pjxq0Bh\n53Mse2Fl9UE/
Gew6IZiRd2OK9yM1xRKH7hjPB3tqFlA98mar+BYAGPhapmq+sSFz\n6TS2ssToUllG8QgJeMxh6+vSP/Ca9O+HiDB7TqE
CufVv6lrL7sfKqfyQ5YzITKm7\nIGDQfdCiorwndvd1i1NB+vviiYsk1fEW8gvRUu7wMRlzmPwxnUxdKmb/b7+O65md
\n7+FlkqU6EzYMQ/224ZJonwJfzmNTO1AGt4aaJDNKn1i5wV22xqqQZvA6nrkBd+06\npUwVTen1AgMBAAECggEAL5D
VVnp0/JhqxMbydptbd613UMqw0bgFdkIgnrKrkIL4\nlsRrpPPHq/4PDzr02C9dd4cNHCQwKzzjv8gHkWDW5U3tEKM2
t6BRs7usdLZqwvOy\naxAfkPTa4BNEe3L1nrR0hTatHxXQRJ1BX3nebn5DliGlbRDwfSVAlwZMYcMjStiS\nZNyS71v
rxRmYFyUNyjGDCZsBDRdSb41cQJ0GmwMd2B8AE5I0spMZm2Y5FM0ZcddX\nlDcELonz1LCTNZaXyhdDBCQ8ecWrSWJZ
8REhTlK/wsTtPbLi1OxIAemcLxzTJQRC\n0tyWzA2zl90hmpJs3of7geGvDCDwRu/MgvuH31MFwQKBgQDxbHm/982/txuB440+
\nMm+x/Ma5HzZg0l8sMdH0wQ5qJYd/lrgz2Ik79FqmFPh0l6LcekA0zGri+4PiRVRx\nAlY9pLFdegIY6jJpvJxJH+kQ00xEd
eUSZ1O0aAn4dlsHaX3wg+SBJ0NiZxsOeQ9m\nrMDKYT7LE3F5indOimDCug2GoQKBgQDLP5FPvA3uWh5Lff14yhVb0T
1oiyeiqe01\nylO7LkCI0s002/M7U0gWXd2XNqAr98KRFtVsbf9gZxsKXTvDI+Vsd1lxGGfNZXmM\nwodSK9zIeL4Ev
e7mRtcB/ZDjtqOn0Um2YeVfXZrEacQoopYo7B4pwjpJmIq/40w3\nOlhXOXEm1QKBgQDPkd9/8LQCwJEy9Q1sS3sDQf
0uDyr2xgkz+0W0NQSKuOeuCE0p\nrmQXmzkREHip7fIFtEpd2t+PdoZm1gsK+uJhL6ebYhpJh5p+lL6elIQThkhNmDu
y\nvgoW01i3OjN7xPSWBSBC9xoVkeaOZAGc2q0Lk96kRXxL7oQzkAAvjD2y4QKBgHEe\neQaSmIJO/8tuXLNsbYTDqN
TVlgKvZoloiT+FV3+PK4y+2dnr2RQxu9GcIns2EsDj\nn3cQpXCHEgKrr0ZFZTwAFy6JscQcNRFFd0Ehjmi44rEK8Lq
TNLkz4f8KuHz/O3JZ\ne+qe0zN71iPzkXVHLOZ65ivtzVNM8y9NtrsdCj/dAoGBAJNM0+Fbt3i1El+U/jOQ\nKwD8vB
VwsJEZ0UspoxETTAnu0sgIUbRECVhn/BQ5ja3HusRaDRsKb7ROLyjnRuC7\nnnR/wM//oENnRm50hEi4Ocfp0eAOx7XQ
OUuE08XhUMyXp00mOCo1NwOFtL0WdG6Bk\nSNV2aPx+2+DGSZEVbuLXviHs\n-----END PRIVATE KEY-----",
      "host": "ip-10-81-125-132.us-west-2.compute.internal",
      "port": "443",
      "distinguishedName": "UID=r-0595a13c153d76ae5,CN=ManagementCA,OU=ami-02a4474c1f74940a8
,O=ip-10-81-125-132.us-west-2.compute.internal",
      "certificateProfile": "ENDUSER",
      "endEntityProfile": "EMPTY"
    }
  }
}
```


Monitoring External CA

Monitoring certificates is done on the same **Orchestrator** > **Certificate Authorities** page.

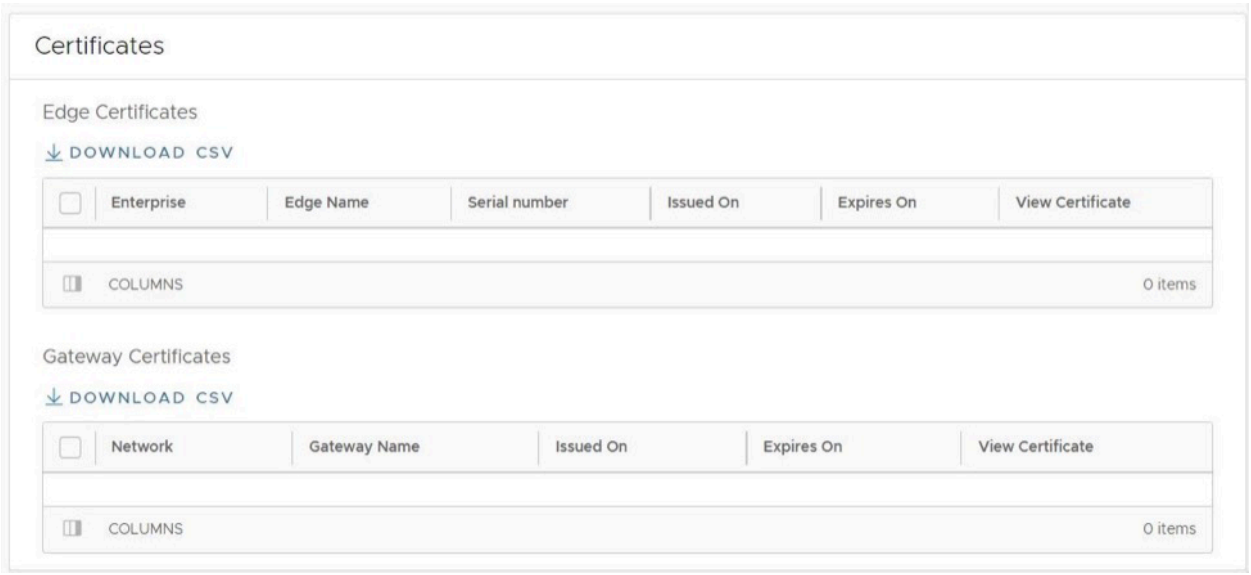
The **Certificates Summary** page provides an Operator with a visual status of key indicators for their certificates' life cycle. The Operator would also import certificates and download CSRs in this section.

Figure 28-13: Monitor Certificates



In the **Certificates** section, the Operator can download a complete list of all Edge or Gateway certificates in the `.csv` format.

Figure 28-14: View Edge and Gateway Certificates



An Operator, Partner, or Customer administrator can also examine a particular Edge's certificate by navigating to **Configure** > **Edge** > **Overview**.

Limitations

- The customer can enable an External CA on an on-premises Orchestrator. This feature is not available on Orchestrator.
- On an Orchestrator using Release 5.0.0, this feature can only use PrimeKey EJBCA PKI as an external CA.

Chapter 29

Appendix

This topic contains the following section:

- Operator-Level Orchestrator Alerts and Events

29.1 Operator-Level Orchestrator Alerts and Events

Discusses a summary of alerts and events generated within the Arista Edge Cloud Orchestrator at the Operator level.

The document provides details about all Operator-level Orchestrator events. Although the Orchestrator stores and displays these events on the UI, the Gateway or one of its running components (such as MGD or PROCMON) generates most of them. The Orchestrator generates only a few specific events itself. The administrator can configure notifications and alerts for these events only within the Orchestrator.

The following table provides an explanation for each of the columns in the **Operator-level Orchestrator Events** table:

Table 78: Operator-level Orchestrator Events

Column name	Details
EVENT	Unique name of the event
DISPLAYED ON ORCHESTRATOR UI AS	Specifies how the event is displayed on the Orchestrator.
SEVERITY	The severity with which this event is usually generated.
GENERATED BY	The VeloCloud SD-WAN component generating the notification can be one of the following: • Orchestrator • Gateway
GENERATED WHEN	Technical reason(s) and circumstances under which this event is generated.
RELEASE ADDED IN	The release this event was first added. If not specified, this event existed prior to release 2.5.
DEPRECATED	Specifies if the event is deprecated from a specific release.

Table 79: Operator-level Orchestrator Events

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPREC.
GATEWAY_UP	Gateway up	INFO	Orchestrator	A Gateway restores after losing connectivity with the Orchestrator.		
GATEWAY_DOWN	Gateway down	INFO	Orchestrator	A Gateway fails to communicate after losing connectivity with the Orchestrator.		
GATEWAY_LARGE_PKT_SIZE	Packet size limit exceeded	INFO	Gateway	The packet size limit incoming from a Gateway's peer exceeded.		
GATEWAY_SERVICE_FAILED	Gateway service failed	ERROR	Gateway	The GWD service on the Gateway fails.		
GATEWAY_BFD _NEIGHBOR_UP	BFD session established to Gateway neighbor	INFO	Gateway	A Gateway BFD neighbor comes back up		
GATEWAY_BFD _NEIGHBOR_DOWN	Gateway BFD neighbor unavailable	INFO	Gateway	A Gateway BFD neighbor comes back down		
GATEWAY_ICMP _PROBE_UNSTABLE	Gateway: ICMP probe unstable	ALERT	Gateway	The ICMP probe goes down on Partner Gateway.		
GATEWAY_REBALANCE	Gateways rebalanced	INFO	Orchestrator			
PROXY_ENABLE_OPERATOR _ACCESS	Partner access delegated to operator	INFO	Orchestrator			
PROXY_DISABLE_OPERATOR _ACCESS	Partner access revoked to operator	INFO	Orchestrator			
VRF_ROUTEMAP_RULE _MAX_LIMIT_HIT	VRF route map rules limit exceeded	WARNING	Gateway	The VRF Inbound/ Outbound route map maximum limit exceeded (32).		
VRF_LIMIT_EXCEEDED	VRF limit exceeded	ALERT	Gateway	The VRF entries configured exceeded maximum limit (1000).		
ENABLE_EXTERNAL_CA	External CA Enabled	CRITICAL	Orchestrator	The `ca.external.enable` property is set to true.	4.3.0	
DISABLE_EXTERNAL_CA	External CA Disabled	CRITICAL	Orchestrator	The `ca.external.enable` property is set to false.	4.3.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPREC.
INSERT_EXTERNAL_CA	External CA Inserted	CRITICAL	Orchestrator	External CA is inserted into the VELOCLOUD _CERTIFICATE _AUTHORITY table and becomes a trusted issuer.	4.3.0	
CREATE_COMPOSITE_ROLE	Composite Role Created	INFO	Orchestrator	A composite role is created by an Enterprise, Partner, or Operator.	4.5.0	
UPDATE_COMPOSITE _ROLE	Composite Role Updated	INFO	Orchestrator	A composite role is updated by an Enterprise, Partner, or Operator.	4.5.0	
DELETE_COMPOSITE_ROLE	Composite Role Deleted	INFO	Orchestrator	A composite role is deleted by an Enterprise, Partner, or Operator.	4.5.0	
CA_VALIDATION	CA validation failure	ALERT	Orchestrator	The CA certificate attributes are rejected.	5.0.0	
EI_ACTIVATION_CONFIG_SENT	EI activation config sent	INFO	Orchestrator	The activation config has been successfully sent to the EI server.	5.0.0	
Auto_Rate_Limit_Enabled	Auto Rate-Limit Enabled	WARNING	Gateway	The Gateway activates the auto rate-limit capability if it detects that specific Edges are sending large volumes of traffic that may destabilize the Gateway or cause packet drops. The resulting event message includes details about the affected Edges, including the Enterprise name and the applied Rate Limit Percentage.	5.2.0	
Auto_Rate_Limit_Disabled	Auto Rate-Limit Disabled	WARNING	Gateway	Gateway auto rate-limit condition is restored.	5.2.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPREC.
SELF_HEALING_REPORT	anomaly_type: <Remote Route inconsistency>, num_routes_recovered: <number>, shr state: <DONE>	ALERT	Gateway	The Gateway generates this event when it detects missing routes in a customer enterprise. The system then corrects the issue by using the Self-Healing Routing feature to recover those routes.	5.2.0	
POLL_IDPS_SIGNATURE_FAIL	Failure in poll job that queries and downloads signature file from GSM	ERROR	Orchestrator	When Orchestrator backend poll job failed to retrieve or download suricata signature from GSM and update profiles with the new signature meta-data.	5.2.0	
IDPS_SIGNATURE_VCO_VERSION_CHECK_FAIL	Querying existing signature version from local DB failed	ERROR	Orchestrator	When Orchestrator backend poll job fails to retrieve existing suricata signature version from Orchestrator's local database.	5.2.0	
IDPS_SIGNATURE_GSM_VERSION_CHECK_FAIL	Querying signature meta-data from GSM failed	ERROR	Orchestrator	When Orchestrator backend poll job fails to retrieve existing suricata signature meta-data (that includes signature version) from GSM.	5.2.0	
IDPS_SIGNATURE_SKIP_DOWNLOAD_NO_UPDATE	Skipping signature download due to no change in signature version	INFO	Orchestrator	When Orchestrator backend poll job skips downloading suricata signature file due to no change in suricata signature file version.	5.2.0	
IDPS_SIGNATURE_STORE_FAILURE_NO_PATH	Filestore path not set to store signature file	ERROR	Orchestrator	When Orchestrator backend poll job fails to store suricata signature file due to filestore path not being set.	5.2.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPREC.
IDPS_SIGNATURE _DOWNLOAD_SUCCESS	Successfully downloaded signature file from GSM	INFO	Orchestrator	When Orchestrator backend poll job successfully downloads suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE _DOWNLOAD_FAILURE	Failed to download signature file from GSM	ERROR	Orchestrator	When Orchestrator backend poll job fails to download suricata signature file from GSM.	5.2.0	
IDPS_SIGNATURE _STORE_SUCCESS	Successfully stored the signature file in filestore	INFO	Orchestrator	When Orchestrator backend poll job successfully stores the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_STORE _SIGNATURE_FAILURE	Failed to store the signature file in filestore	ERROR	Orchestrator	When Orchestrator backend poll job fails to store the suricata signature file in local file store.	5.2.0	
IDPS_SIGNATURE_METADATA _INSERT_SUCCESS	Successfully added meta-data of the signature file to local DB	INFO	Orchestrator	When Orchestrator backend poll job successfully adds meta-data of the suricata signature file to local DB.	5.2.0	
IDPS_SIGNATURE_METADATA _INSERT_FAILURE	Failure to add meta-data of the signature file to local DB	ERROR	Orchestrator	When Orchestrator backend poll job fails to add meta-data of the suricata signature file to local DB.	5.2.0	
POLL_URL_CATEGORIES _FAIL	POLL_URL_CATEGORIES _FAIL	ERROR	Orchestrator	Generated when Orchestrator URL categories poll job fails.	6.0.0	
URL_CATEGORIES_STORE _SUCCESS	URL_CATEGORIES_STORE _SUCCESS	INFO	Orchestrator	Generated when Orchestrator URL categories are stored successfully.	6.0.0	
URL_CATEGORIES_STORE_FAILURE	URL_CATEGORIES_STORE _FAILURE	ERROR	Orchestrator	Generated when Orchestrator URL categories storage job fails.	6.0.0	

EVENT	DISPLAYED ON ORCHESTRATOR UI AS	SEVERITY	GENERATED BY	GENERATED WHEN	RELEASE ADDED IN	DEPREC.
VCO_ENTERPRISE_NTICS _LICENSE_REQUEST_FAILED	VCO_ENTERPRISE_NTICS _LICENSE_REQUEST_FAILED	ERROR	Orchestrator	Generated when Orchestrator Enterprise NTICS license request fails.	6.0.0	
VCO_ENTERPRISE_NTICS _LICENSE_REQUEST_SUCCEEDED	NTICS License request succeeded	INFO	Orchestrator	Generated when Orchestrator Enterprise NTICS license request succeeds.	6.0.0	

Gateway Capacity Events

Currently, the system assigns Gateways based on Geo-proximity and does not consider Gateway capacity health metrics. To improve Edge-to-Gateway assignment, the system periodically monitors capacity health metrics based on warning and critical thresholds. These metrics include:

- **Edge Count** and **Tunnel Count**
- **PKI Activated Tunnel Count**
- **Flow Count** and **NAT Count**
- **Packet Queue Watermark** and **Packet Drops**

When any metric exceeds the defined thresholds, the Gateway generates capacity events and reports them to the Orchestrator. These events provide Operators and Partners clear visibility into Gateway health, allowing them to make intelligent and accurate Gateway assignments.

The following are the Gateway capacity events generated based on the capacity threshold limits.

Table 80: Gateway Capacity Events

Metric	Trigger	Event	Severity	Message	Event Detail
Edge Count	Above Warning Threshold. The Warning threshold value is 90% of following Supported values: • 4 CPU, 32G MEM - 2000 • 8 CPU, 32G MEM - 4000	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of connected Edges as Gateway has crossed warning threshold.	• 4 CPU: The number of connected Edges is above the warning threshold (1800). • 8 CPU: The number of connected Edges is above the warning threshold (3600).
Edge Count	Above Critical Threshold. The Critical threshold value is 95% of following Supported values: • 4 CPU, 32G MEM - 2000 • 8 CPU, 32G MEM - 4000	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of connected Edges as Gateway has crossed critical threshold.	• 4 CPU: The number of connected Edges is above the critical threshold (1900). • 8 CPU: The number of connected Edges is above the critical threshold (3800).
Edge Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of connected Edges restored.	The number of connected Edges is within the acceptable threshold.
Tunnel Count	Above Warning Threshold. The Warning threshold value is 90% of following Supported values: • 4 CPU, 32G MEM - 3000 • 8 CPU, 32G MEM - 6000	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of tunnels.	• 4 CPU: The number of tunnels is above the warning threshold (2700). • 8 CPU: The number of tunnels is above the warning threshold (5400).
Tunnel Count	Above Critical Threshold. The Critical threshold value is 95% of following Supported values: • 4 CPU, 32G MEM- 3000 • 8 CPU, 32G MEM- 6000	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of tunnels.	• 4 CPU: The number of tunnels is above the critical threshold (2850). • 8 CPU: The number of tunnels is above the critical threshold (5700).
Tunnel Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of tunnels restored.	The number of tunnels is within the acceptable threshold.
Flow Count	Above Warning Threshold. The Warning threshold value is 50% of Supported value 1920000.	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of flows.	The number of flows is above the warning threshold (960000).
Flow Count	Above Critical Threshold. The Critical threshold value is 75% of Supported value 1920000.	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of flows.	The number of flows is above the critical threshold (1440000)
Flow Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of flows restored.	The number of flows is within the acceptable threshold.
NAT Entries Count	Above Warning Threshold. The Warning threshold value is 50% of Supported value 1920000.	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of NAT entries.	The number of NAT entries is above the warning threshold (960000).

Metric	Trigger	Event	Severity	Message	Event Detail
NAT Entries Count	Above Critical Threshold. The Critical threshold value is 75% of Supported value 1920000.	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of NAT entries.	The number of NAT entries is above the critical threshold (1440000).
NAT Entries Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of NAT entries restored.	The number of NAT entries is within the acceptable threshold.
Packet Queue Watermark	Above Critical Threshold	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high packet queue watermark.	The packet queue watermark is above the critical threshold (6000) for 5 consecutive seconds.
Packet Queue Watermark	Above Warning Threshold	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high packet queue watermark.	The packet queue watermark is above the warning threshold (2000) for 10 consecutive seconds.
Packet Queue Watermark	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high packet queue watermark restored.	The packet queue watermark is within the acceptable threshold.
Packet Drop Count	Above Critical Threshold	GATEWAY_CRITICAL	NOTICE	Over capacity alert due to high number of packet drops.	The number of packet drops is above the critical threshold (2000) for 5 consecutive seconds.
Packet Drop Count	Above Warning Threshold	GATEWAY_DEGRADED	NOTICE	Over capacity alert due to high number of packet drops.	The number of packet drops is above the warning threshold (500) for 10 consecutive seconds.
Packet Drop Count	Below Warning Threshold	GATEWAY_STABLE	INFO	Over capacity condition due to high number of packet drops restored.	The number of packet drops is within the acceptable threshold.

Chapter 30

References

This topic contains the following section:

- Related Documents

30.1 Related Documents

Arista provides the following documentation for **VeloCloud SD-WAN**:

- *Arista VeloCloud SD-WAN Administration Guide*
- *Arista VeloCloud SD-WAN Partner Guide*
- *Arista VeloCloud SD-WAN Gateway Monitoring Guide*
- *Arista VeloCloud SD-WAN Orchestrator Deployment and Monitoring Guide*
- *Arista VeloCloud SD-WAN Troubleshooting Guide*
- *Arista VeloCloud SASE Global Settings Guide*
- *Arista VeloCloud SD-WAN Design Guide for Enhanced Firewall Services*
- *Arista VeloCloud SD-WAN 6.4 API*
- *Arista VeloCloud Portal API 6.4*